Vereinbarung über die Verarbeitung personenbezogener Daten im Auftrag nach Art. 28 DSGVO

zwischen

____

____

- als Verantwortlicher - nachstehend Auftraggeber genannt -

und

H2 Invent GmbH
Gewerbestraße 9, 79539 Lörrach

– als Auftragsverarbeiter - nachstehend Auftragnehmer genannt -

H2 invent ist spezialisiert auf die digitale Transformation bestehender Prozesse von kleinen, mittleren und großen Unternehmen sowie Non-Profit-Organisationen und öffentlichen Institutionen.

H2 invent legt großen wert auf digitale Suveränität und IT Sicherheit. Um dies zu erreichen, entwickelt H2 invent eigene Open-Source Anwendungen oder setzt Open-Source Software ein, die zusammen mit den Maintainern weiterenwickelt und optimiert wird. Um die IT Sicherheit heute und morgen zu gewähren, entwickeln H2 invent täglich an Updates, neuen Funktionen, optimiert die Konfigurationen der Server und Anwendungen und führt interne Sicherheitstests durch.

§ 1 Allgemeines

(1) Der Auftragnehmer erbringt Dienstleistungen, welche im Einzelnen in Ziff. 3 und **Anlage 1** beschrieben sind.

(2) Der Auftragnehmer verarbeitet personenbezogene Daten des Auftraggebers im Sinne von Art. 4 Nr. 8 und Art. 28 der Verordnung (EU) 2016/679 – Datenschutzgrundverordnung, kurz DSGVO. Dieser Vertrag regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung personenbezogener Daten im Auftrag.

§ 2 Definitionen

(1) Verantwortlicher ist gem. Art. 4 Nr. 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 Nr. 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 Nr. 11 DSGVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) 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, identifiziert werden kann.

(4) Besonders schutzbedürftige personenbezogene Daten sind personenbezogene Daten gem. Art. 9 DSGVO, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit von Betroffenen hervorgehen, sowie Gesundheitsdaten gem. Art. 4 Nr. 15 DSGVO.

(5) Verarbeitung ist gem. Art. 4 Nr. 2 DSGVO jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten

Initials ________

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.

§ 3 Gegenstand und Dauer des Auftrags

(1) Gegenstand der Verarbeitung

Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst alle Tätigkeiten, die der Auftragnehmer gemäß den Leistungsbeschreibungen und den jeweiligen vertraglichen Vereinbarungen mit dem Auftraggeber erbringt und die eine Auftragsverarbeitung darstellen. Der Gegenstand des Auftrags im Einzelnen ergibt sich aus der Leistungsvereinbarung gem. **Anlage 1** (Beschreibung der Dienstleistungen). Dies gilt auch, sofern die Leistungsbeschreibungen und die jeweiligen vertraglichen Vereinbarungen nicht ausdrücklich Bezug nehmen auf diese Vereinbarung zur Auftragsverarbeitung.

(2) Dauer der Verarbeitung

Die Verarbeitung erfolgt zeitlich unbefristet, sofern dies nicht anders vereinbart ist. Die in den jeweiligen vertraglichen Leistungsvereinbarungen geregelten Kündigungsfristen bleiben unberührt. Soweit nicht abweichend vereinbart, kann der Auftrag von beiden Parteien mit einer Frist von 3 Monaten zum Monatsende gekündigt werden. Mit Kündigung der Leistungsvereinbarung endet automatisch diese Auftragsvereinbarung. Die Möglichkeit zur fristlosen Kündigung aus wichtigem Grund bleibt hiervon unberührt.

§ 4 Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten, Ort der Verarbeitung

Die Art der Verarbeitung umfasst alle Arten von Verarbeitungen im Sinne der DSGVO, welche für die Auftragsverarbeitung erforderlich sind. Der Zweck der Verarbeitung personenbezogener Daten ist in **Anlage 1** (Beschreibung der Dienstleistungen) definiert. Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union statt. Ziff. 9 Abs. 2 bleibt unberührt.

(2) Art der Daten

Arten der personenbezogenen Daten sind alle Arten personenbezogener Daten, die der Auftragnehmer im Auftrag des Auftraggebers verarbeitet. Hiervon umfasst sind auch besondere Kategorien personenbezogener Daten. Gegenstand der Verarbeitung personenbezogener Daten sind insbesondere folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien). Die Einzelheiten sind in **Anlage 1** beschrieben.

(3) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen sind in **Anlage 1** beschrieben.

§ 5 Verpflichtung zur Vertraulichkeit

Der Auftragnehmer gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit und zur Einhaltung der Anforderungen nach der DSGVO verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b) DSGVO.

Die Vertraulichkeits-/Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

§ 6 Technisch und organisatorische Maßnahmen (TOM)

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c), 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen. Die Einzelheiten sind in **Anlage 2** geregelt.

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsni-

veau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

§ 7 Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Der Auftragnehmer verzichtet auf ein Zurückbehaltungsrecht nach § 273 BGB an den Daten.

§ 8 Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

(1) Der Auftragnehmer ist zur Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b), 29, 32 Abs. 4 DSGVO verpflichtet. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

(2) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c), 32 DSGVO ist in **Anlage 2** geregelt.

(3) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

(4) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

(5) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird. Die Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber erfolgt im Rahmen seiner Kontrollbefugnisse nach Ziffer 10 dieses Vertrages.

(6) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikel 32 - 36 genannten Pflichten nach Maßgabe von Art. 28 Abs. 3 lit. f) DSGVO.

(7) Soweit gesetzlich verpflichtet, bestellt der Auftragnehmer eine fachkundige und zuverlässige Person als Beauftragten für den Datenschutz. Weitere Informationen dazu stehen in **Anlage 1**.

§ 9 Unterauftragsverhältnisse

(1) Der Auftragnehmer setzt derzeit die in **Anlage 1** genannten Unterauftragnehmer ein.

(2) Der Auftraggeber erteilt dem Auftragnehmer die grundsätzliche Genehmigung weitere Unterauftragnehmer in Anspruch zu nehmen. Die Auslagerung auf weitere Unterauftragnehmer oder der Wechsel bestehender Unterauftragnehmer sind zulässig, soweit kumulativ:

a) der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit von mindestens 4 Wochen vorab schriftlich oder in Textform anzeigt,

b) der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform wegen eines wichtigen Grundes Einspruch gegen die geplante Auslagerung erhebt und

c) eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zugrunde gelegt wird.

(2) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR, stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen und Garantien nach Art. 44 ff. DSGVO sicher. Die Beauftragung von Unterauftragnehmer in Drittländer ist nur mit vorheriger schriftlicher Zustimmung des Auftraggebers zulässig.

Initials ________

(3) Erteilt der Auftragnehmer Aufträge an weitere Auftragsverarbeiter, so obliegt es dem Auftragnehmer seine datenschutzrechtlichen Pflichten aus diesem Vertrag auf den weiteren Auftragsverarbeiter zu übertragen.

§ 10 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

§ 11 Unterstützungspflichten des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen.

b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden.

c) die Verpflichtung, den Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen.

d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung

e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine angemessene Vergütung beanspruchen.

§ 12 Weisungsbefugnis des Auftraggebers

(1) Der Auftraggeber ist für die Einhaltung der gesetzlichen Bestimmungen des Datenschutzrechts, insbesondere für die Rechtmäßigkeit der Verarbeitung sowie für die Wahrung der Betroffenenrechte verantwortlich. Gesetzliche oder vertragliche Haftungsregelungen bleiben hiervon unberührt.

(2) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(3) Der Auftragnehmer verarbeitet die ihm zur Verfügung gestellten personenbezogenen Daten ausschließlich nach den dokumentierten Weisungen des Auftraggebers und im Rahmen der getroffenen Vereinbarungen. Daten dürfen nur berichtigt, gelöscht und gesperrt werden, wenn der Auftraggeber dies anweist.

(4) Die Verarbeitung erfolgt nur auf Weisung des Auftraggebers, es sei denn, der Auftragnehmer ist durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, zur Verarbeitung dieser Daten verpflichtet. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine Mitteilung nicht wegen eines wichtigen öffentlichen Interesses untersagt.

(5) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber verbindlich bestätigt oder geändert wird.

(6) Soweit zutreffend und vereinbart gilt: Nur die folgenden namentlich genannten Personen (oder deren Vertreter, soweit vereinbart) sind für den Auftraggeber weisungsberechtigt: In **Anlage 1** beschrieben.

§ 13 Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der Erbringung der Verarbeitungsleistungen löscht der Auftragnehmer nach Wahl des Kunden entweder alle personenbezogenen Daten oder gibt sie dem Kunden zurück, sofern nicht nach dem Unionsrecht oder nach deutschem Recht eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht oder sich aus den Leistungsbeschreibungen und den jeweiligen vertraglichen Vereinbarungen etwas anderes ergibt.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

§ 14 Aufsichtsbehörde

Die für den Auftragnehmer zuständige Aufsichtsbehörde ist:

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit
Postanschrift:

Postfach 10 29 32, 70025 Stuttgart

Tel.: 0711/615541-0, FAX: 0711/615541-15, E-Mail: poststelle@lfdi.bwl.de

§ 15 Salvatorische Klausel

Sollten sich einzelne Bestimmungen dieser Vereinbarung als ungültig erweisen, so wird hierdurch die Gültigkeit der übrigen Bestimmungen nicht berührt. Die ungültige Bestimmung ist durch eine solche Regelung zu ersetzen, die die Parteien getroffen hätten, hätten sie bei Abschluss des Vertrags an die Ungültigkeit des jeweiligen Punktes gedacht. Soweit diese Vereinbarung eine unbewusste Regelungslücke enthält, ist diese durch eine solche Regelung zu ersetzen, die die Parteien getroffen hätten, hätten sie bei Abschluss des Vertrags an die Regelungsbedürftigkeit des jeweiligen Punktes gedacht.

§ 16 Formerfordernis

Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – sind gemäß DSGVO schriftlich abzufassen, was auch in einem elektronischen Format 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.

§ 17 Schlussbestimmungen

(1) Auf diese Auftragsverarbeitung und alle in diesem Zusammenhang erbrachten Verarbeitungstätigkeiten findet deutsches Recht Anwendung.

(2) Gerichtsstand für alle Streitigkeiten aus oder im Zusammenhang mit dieser Vereinbarung, gleich aus welchem Rechtsgrund, ist Freiburg i.Br., Deutschland.

(3) Änderungen dieser Vereinbarung bedürfen der Schriftform. Das gilt auch für die Aufhebung des Schriftformerfordernisses.

(4) Sollten Bestimmungen dieser Vereinbarung unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. In diesem Fall ist die unwirksame Bestimmung durch die gesetzliche/n Regelung/en zu ersetzen.

Initials ________

Die folgenden Anlagen sind zum Zeitpunkt der Vertragaunterzeichnung integraler Bestandteil dieser Vereinbarung

Anlage 1 – Beschreibung der Dienstleistungen, Art der Daten, Kategorien der betroffenen Personen, weisungsberechtigte Personen des Auftraggebers, Unterauftragnehmer

Anlage 2 – Technisch-organisatorische Maßnahmen

Auftraggeber (Verantwortlicher)	**H2 Invent GmbH (Auftragnehmer, AV)**
……..……., den ______________________	Lörrach, den 11.07.2024
	H2 invent Gewerbestraße 9 79539 Lörrach
___________________________________	___________________________________
(Unterschrift/en, Stempel)	(Unterschrift/en, Stempel)

Initials ________