# Vereinbarung zur Auftragsverarbeitung

zwischen

als Verantwortlicher (nachfolgend „Verantwortlicher"),

und

**Varify Software GmbH**, Südliche Münchner Straße 55, 82031 Grünwald, Deutschland

als Auftragsverarbeiter (nachfolgend „Auftragsverarbeiter",
Verantwortlicher und Auftragsverarbeiter gemeinsam die „Parteien")

## Präambel

Der Verantwortliche hat den Auftragsverarbeiter in den allgemeinen Geschäftsbedingungen (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 ist die nachfolgende Vereinbarung zur Auftragsverarbeitung (nachfolgend „Vereinbarung“) Teil des Hauptvertrages, 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 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, personenbezogene Daten gem. Art. 10 DSGVO über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln sowie genetische Daten gem. Art. 4 Abs. 13 DSGVO, biometrische 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, der 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. Weitere Informationen der Datenverarbeitung durch den Auftragsverarbeiter ergeben sich aus Anlage 1, dem Hauptvertrag und etwaigen zugehörigen Leistungsbeschreibungen. 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.

(5) Der Auftragsverarbeiter bietet dem Verantwortlichen optional KI-gestützte Funktionen an. Die Nutzung dieser Funktionen ist freiwillig und erfordert eine gesonderte Aktivierung durch den jeweiligen Nutzer. Vor der erstmaligen Nutzung wird der Nutzer darauf hingewiesen, dass Eingaben an Drittanbieter-KI-Dienste übermittelt werden können, und stimmt zu, keine personenbezogenen Daten einzugeben. Der Auftragsverarbeiter überträgt im Rahmen der KI-Funktionen selbst keine personenbezogenen Daten an die in Anlage 5 unter A5.3 bis A5.6 genannten Dienste. Die Verantwortung für die Inhalte der Eingaben liegt beim Verantwortlichen bzw. dem jeweiligen Nutzer.

## § 3 Weisungsrecht

(1) Der Auftragsverarbeiter darf Daten nur im Rahmen des Hauptvertrags und gemäß den Weisungen des Verantwortlichen erheben, verarbeiten oder nutzen. 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, Drittland

(1) Im Rahmen der Durchführung des Hauptvertrags erhält der Auftragsverarbeiter Zugriff auf die in Anlage 2 näher spezifizierten personenbezogenen Daten.

(2) Der Kreis der von der Datenverarbeitung Betroffenen ist in Anlage 3 dargestellt.

(3) Eine Weitergabe personenbezogener Daten in ein Drittland (außerhalb des EWR) darf unter den Voraussetzungen der Art. 44 ff. DSGVO stattfinden.

(4) Die Parteien vereinbaren, dass, soweit personenbezogene Daten ohne Angemessenheitsentscheidung gemäß Art. 45 DSGVO in ein Drittland übertragen werden, die Standardvertragsklauseln (Modul 2 – Verantwortlicher an Auftragsverarbeiter) gemäß der Durchführungsentscheidung der Europäischen Kommission (EU) 2021/914 hiermit durch Verweisung in diesen Vertrag aufgenommen werden und gelten. In solchen Fällen ist der Verantwortliche der Datenexporteur und der Auftragsverarbeiter der Datenimporteur. Die aufgenommenen Klauseln sind ein integraler Bestandteil dieses Vertrags.

(5) Übermittlungen personenbezogener Daten an Unterauftragsverarbeiter in Drittländern erfolgen auf Grundlage eines Angemessenheitsbeschlusses oder, soweit ein solcher nicht besteht, auf Grundlage der Standardvertragsklauseln (Modul 3 – Auftragsverarbeiter an Auftragsverarbeiter), die der Auftragsverarbeiter mit dem jeweiligen Unterauftragsverarbeiter abschließt. Einzelheiten ergeben sich aus Anlage 5.

## § 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 4 genannten technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Verantwortlichen gem. Art. 32 DSGVO getroffen, die der Verantwortliche als angemessen anerkennt. Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Dazu werden die Schutzziele von Art. 32 Abs. 1 DSGVO, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird. 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 Martin Bastius, heyData GmbH, Schützenstraße 5, 10117 Berlin, E-Mail: datenschutz@heydata.eu, www.heydata.eu. Dieselbe Angabe findet sich in Anlage 4, Ziffer A4.1.1.

## § 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 Dienstleistern

(1) Die vertraglich vereinbarten Leistungen werden unter Einschaltung der in Anlage 5 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 vor jeder beabsichtigten 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 Erhalt der Information über die Änderung 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 Auftragsverarbeiter 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.

(3) Soweit zutreffend und in dem Maße, wie der Auftragsverarbeiter personenbezogene Daten von kalifornischen Einwohnern im Auftrag des Verantwortlichen verarbeitet, handelt der Auftragsverarbeiter als „Dienstleister“ im Sinne von §1798.140(v) des California Consumer Privacy Act (CCPA/CPRA) und darf solche personenbezogenen Daten nicht verkaufen oder teilen, wie darin definiert.

## § 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 allein 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 vertragsgemäße 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 Auftragsverarbeiter 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.

(5) Im Falle eines Konflikts zwischen diesem Vertrag und den aufgenommenen Standardvertragsklauseln haben letztere Vorrang für den Zweck der grenzüberschreitenden Datenübertragungen.

## Verantwortlicher

Name:

Position:

## Auftragsverarbeiter

Name: Steffen Schulz

Position: CEO

Datum:

Unterschriften:

| | |
|---|---|
| _____ | _____ |
| Verantwortlicher | Auftragsverarbeiter |

# Anlagen

## Anlage 1 – Gegenstand der Auftragsverarbeitung

Durchführung von A/B-Tests zur Optimierung und Verbesserung von Webdiensten, Software, Benutzeroberflächen oder anderen digitalen Produkten.

Optional: Bereitstellung KI-gestützter Funktionen zur Unterstützung der Webseitenoptimierung, deren Nutzung eine gesonderte Aktivierung durch den Nutzer erfordert.

Optional: Auswertung der Testergebnisse über das Varify Realtime Tracking, dessen Nutzung eine Freischaltung im Account des Verantwortlichen erfordert.

## Anlage 2 – Beschreibung der Daten/Datenkategorien

- Netzwerkdaten: Quell- und Ziel-IP-Adressen, Netzwerkverkehrsdetails
- Log-Daten: Metadaten zu Netzwerkereignissen (z. B. Anfragen an Websites, Anwendungen oder APIs), Informationen über Besucher oder autorisierte Benutzer
- Geolokalisierungsdaten: Abgeleitet aus IP-Adressen, um Anfragen an den nächstgelegenen Server zu leiten
- Browser- und Geräteinformationen: Informationen, die verwendet werden, um Inhalte basierend auf Gerät und Browser des Nutzers zu optimieren

## Anlage 3 – Beschreibung der Betroffenen/Betroffenengruppen

Nutzer von Webseiten und/oder Mobile-Apps, die varify.io einsetzen

## Anlage 4 – Technische und organisatorische Maßnahmen des Auftragsverarbeiters

Es gelten ausschließlich die in dieser Anlage 4 aufgeführten technischen und organisatorischen Maßnahmen. Ein separates Dokument mit technischen und organisatorischen Maßnahmen existiert nicht.

### A4.1 Einleitung

#### A4.1.1 Datenschutzbeauftragter

Unser Datenschutzbeauftragter ist Martin Bastius, heyData GmbH, Schützenstraße 5, 10117 Berlin, E-Mail: datenschutz@heydata.eu, www.heydata.eu. Dieselbe Angabe findet sich in § 5 Abs. 4 dieses Vertrages.

#### A4.1.2 Gegenstand des Dokuments

Dieses Dokument fasst die vom Auftragsverarbeiter getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 Abs. 1 DSGVO zusammen. Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet.

### A4.2 Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

#### A4.2.1 Zutrittskontrolle

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

- Arbeit im Home Office: Anweisung an Mitarbeiter, wenn möglich, in von Wohnräumen abgetrennten Arbeitszimmer zu arbeiten
- Manuelles Schließsystem (z.B. Schlüssel)
- Schlüsselregelung / Schlüsselbuch
- Berechtigungsvergabe ist auf ein Mindestmaß reduziert
- Videoüberwachung der Zugänge
- Umzäunung des Betriebsgeländes
- Besucher nur mit Begleitung von Mitarbeitern
- Gesicherte Einfahrtstore
- Türen mit Knauf auf der Außenseite
- Empfang / Rezeption
- Anweisung an Mitarbeiter, nicht in öffentlich zugänglichen Räumlichkeiten (z.B. Cafés) zu arbeiten

#### A4.2.2 Zugangskontrolle

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

- Unternehmens-Richtlinie „Clean Desk“
- Authentifikation mit Benutzer und Passwort
- Verpflichtende Multi-Faktor-Authentifizierung (MFA) für alle Unternehmenszugänge
- Geregeltes Berechtigungsmanagement und Benutzerverwaltung
- Einsatz von Firewalls
- Einsatz von Antivirensoftware
- Virtuelle Mandantentrennung
- Automatische Bildschirmsperre mit Passwortaktivierung

#### A4.2.3 Zugriffskontrolle

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

- Anweisung an Mitarbeiter, dass nur unbedingt erforderliche Daten ausgedruckt werden
- Anweisung keine externen Datenträger anzuschließen
- Regelungen zur Verwaltung von Benutzerrollen
- Regelmäßige Überprüfung und Protokollierung der Berechtigungen
- Verschlüsselung von mobilen Geräten und Datenträgern

#### A4.2.4 Trennungskontrolle

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

- Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder nach Ablauf der gesetzlichen Löschfrist, wenn möglich, zu anonymisieren/pseudonymisieren.
- Mandantenfähiges System
- Erstellung eines Berechtigungskonzepts
- Versehen der Datensätze mit Zweckattributen/Datenfeldern
- Trennung von Entwicklungs-, Test- und Produktivsystem
- Trennung von Test- und Produktivdaten

### A4.3 Integrität (Art. 32 Abs. 1 lit. b DSGVO)

#### A4.3.1 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)
- E-Mail-Verschlüsselung
- Bereitstellung von Daten über verschlüsselte Verbindungen wie SFTP oder HTTPS
- Protokollierung von Zugriffen und Abrufen

#### A4.3.2 Eingabekontrolle

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

- Klare Zuständigkeiten für Löschungen
- 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
- Datenverarbeitungen geschehen nur auf Anweisung

### A4.4 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:

- Regelmäßige Backups
- Back-up Konzept mit Datensicherung
- Festplattenspiegelung
- Brandschutzkonzept
- Klimatisierungssysteme
- Feuer- und Rauchmeldeanlagen
- Hosting (jedenfalls der wichtigsten Daten) mit einem professionellen Hoster
- Regelmäßige Überprüfung der Systeme auf Sicherheitsschwachstellen
- Monitoring aller relevanten Server
- Maßnahmen gegen DDoS-Attacken
- Patch- und Vulnerability-Management

### A4.5 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

(Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

### A4.5.1 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), die regelmäßig aktualisiert wird
- Kontrolle und regelmäßige Prüfung der technischen und organisatorischen Maßnahmen
- Jährliche Audits/Reviews
- Prozess zum Umgang mit Betroffenenrechten
- Löschkonzepte
- Berechtigungskonzepte

### A4.5.2 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

### A4.5.3 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.

### A4.5.4 Auftragskontrolle

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

- Es bestehen schriftliche Verträge mit Unterauftragsverarbeitern
- Weisungserteilungen sind klar geregelt
- Daten werden spätestens nach Vertragsende gelöscht

- 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)
- Unterauftragsverarbeiter sind sorgsam ausgewählt

## Anlage 5 – Aktuelle Subunternehmer

### A5.1 Amazon AWS

| | |
|---|---|
| **Name:** | Amazon AWS |
| **Anschrift:** | Amazon Web Services EMEA Sàrl, Avenue John F. Kennedy 38, 1855 Luxemburg, Luxemburg |
| **Beschreibung der Verarbeitung:** | AWS mit dem Rechenzentrum in Frankfurt dient als Hosting-Plattform, um die gehostete Software und deren Daten zu speichern und zu verwalten. |
| **Betroffene Datenkategorien:** | Netzwerkdaten: Quell- und Ziel-IP-Adressen, Netzwerkverkehrsdetails |
| **Ort der Verarbeitung:** | Datacenter Frankfurt |
| **Datenschutzrechtliches Vertragsverhältnis:** | Es besteht ein Angemessenheitsbeschluss (das Data Privacy Framework) und der Anbieter ist entsprechend zertifiziert. Für den Fall, dass der Beschluss wegfällt, wurden Standardvertragsklauseln abgeschlossen. |

### A5.2 Cloudflare

| | |
|---|---|
| **Name:** | Cloudflare |
| **Anschrift:** | Cloudflare, Inc., 101 Townsend St, San Francisco, CA 94107, USA |
| **Beschreibung der Verarbeitung:** | Cloudflare wird eingesetzt, um Serveranfragen zwischenzuspeichern, um dadurch die Antwortzeiten zu verbessern und Hosting-Kosten zu reduzieren. |
| **Betroffene Datenkategorien:** | IP-Adressen, Log-Daten (Metadaten zu Netzwerkereignissen), Geolokalisierungsdaten (abgeleitet aus IP-Adressen), Browser- und Geräteinformationen |
| **Ort der Verarbeitung:** | Global, abhängig vom Standort des Nutzers |
| **Datenschutzrechtliches Vertragsverhältnis:** | Es besteht ein Angemessenheitsbeschluss (das Data Privacy Framework) und der Anbieter ist entsprechend zertifiziert. Für den Fall, dass der Beschluss wegfällt, wurden Standardvertragsklauseln abgeschlossen. |

***Hinweis: Die nachfolgenden Unterauftragnehmer A5.3 bis A5.6 kommen ausschließlich bei Nutzung der optionalen AI-Dienste des Auftragsverarbeiters zum Einsatz. Sofern der Verantwortliche keine AI-Funktionen aktiviert oder nutzt, findet keine Datenverarbeitung durch diese Unterauftragnehmer statt.***

### A5.3 Anthropic (Claude) – AI-Dienst

| | |
|---|---|
| **Name:** | Anthropic (Claude) |
| **Anschrift:** | Anthropic, PBC, 548 Market St, PMB 90375, San Francisco, CA 94104, USA |
| **Beschreibung der Verarbeitung:** | Bereitstellung von KI-gestützten Sprachmodellen (Claude) zur Verarbeitung von Texteingaben und Generierung von Textausgaben im Rahmen optionaler AI-Funktionen des Auftragsverarbeiters. |
| **Betroffene Datenkategorien:** | Texteingaben des Nutzers (Prompts), die ggf. personenbezogene Daten enthalten können; generierte Textausgaben |
| **Ort der Verarbeitung:** | USA (Google Cloud / AWS Rechenzentren) |
| **Datenschutzrechtliches Vertragsverhältnis:** | Data Processing Addendum (DPA) mit Anthropic abgeschlossen. Standardvertragsklauseln gem. EU 2021/914 vereinbart. Zero Data Retention (keine Speicherung der API-Eingaben für Trainings). |

### A5.4 OpenAI (Codex) – AI-Dienst

| | |
|---|---|
| **Name:** | OpenAI (Codex) |
| **Anschrift:** | OpenAI, L.L.C., 3180 18th Street, San Francisco, CA 94110, USA |
| **Beschreibung der Verarbeitung:** | Bereitstellung von KI-gestützten Sprachmodellen (Codex) zur automatisierten Code-Generierung und Textverarbeitung im Rahmen optionaler AI-Funktionen des Auftragsverarbeiters. |
| **Betroffene Datenkategorien:** | Texteingaben des Nutzers (Prompts), die ggf. personenbezogene Daten enthalten können; generierte Textausgaben |
| **Ort der Verarbeitung:** | USA (Microsoft Azure Rechenzentren) |
| **Datenschutzrechtliches Vertragsverhältnis:** | Data Processing Addendum (DPA) mit OpenAI abgeschlossen. Es besteht ein Angemessenheitsbeschluss (das Data Privacy Framework) und der Anbieter ist entsprechend zertifiziert. Standardvertragsklauseln vereinbart. Zero Data Retention (keine Speicherung der API-Eingaben für Trainings). |

### A5.5 Google (Gemini) – AI-Dienst

| | |
|---|---|
| **Name:** | Google (Gemini) |
| **Anschrift:** | Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland |
| **Beschreibung der Verarbeitung:** | Bereitstellung von KI-gestützten Sprachmodellen (Gemini) zur Verarbeitung von Texteingaben und Generierung von |

| | |
|---|---|
| | Textausgaben im Rahmen optionaler AI-Funktionen des Auftragsverarbeiters. |
| **Betroffene Datenkategorien:** | Texteingaben des Nutzers (Prompts), die ggf. personenbezogene Daten enthalten können; generierte Textausgaben |
| **Ort der Verarbeitung:** | EU/EWR (Google Cloud Rechenzentren, u.a. Irland, Niederlande, Finnland); ggf. USA |
| **Datenschutzrechtliches Vertragsverhältnis:** | Google Cloud Data Processing Addendum (DPA) abgeschlossen. EU-Rechenzentren verfügbar. Für Drittlandtransfers: Angemessenheitsbeschluss (Data Privacy Framework) und Standardvertragsklauseln vereinbart. |

### A5.6 Firecrawl (SideGuide Technologies, Inc.)

| | |
|---|---|
| **Name:** | Firecrawl (SideGuide Technologies, Inc.) |
| **Anschrift:** | SideGuide Technologies, Inc. d/b/a Firecrawl, 800 Haight Street, San Francisco, CA, USA |
| **Beschreibung der Verarbeitung:** | Bereitstellung einer Web-Scraping- und Datenextraktions-API zur Aufbereitung von Webinhalten für KI-gestützte Funktionen im Rahmen optionaler AI-Dienste des Auftragsverarbeiters. Firecrawl extrahiert öffentlich zugängliche Webinhalte und wandelt diese in strukturierte Daten um. |
| **Betroffene Datenkategorien:** | URLs und Webinhalte öffentlich zugänglicher Webseiten; ggf. auf diesen Seiten enthaltene personenbezogene Daten (z. B. Impressumsdaten, Kontaktinformationen) |
| **Ort der Verarbeitung:** | USA (Cloud-Infrastruktur) |
| **Datenschutzrechtliches Vertragsverhältnis:** | Nutzung gemäß Firecrawl Terms of Service. Es werden ausschließlich öffentlich zugängliche Webinhalte verarbeitet. Standardvertragsklauseln für Drittlandtransfers vereinbart. |

***Hinweis: Der nachfolgende Unterauftragnehmer A5.7 kommt ausschließlich zum Einsatz, wenn der Verantwortliche seine Testergebnisse mit dem Varify Realtime Tracking auswertet. Dieser Dienst ist optional und muss im Account des Verantwortlichen freigeschaltet werden. Ohne Freischaltung findet keine Datenverarbeitung durch diesen Unterauftragnehmer statt.***

### A5.7 ClickHouse

| | |
|---|---|
| **Name:** | ClickHouse |
| **Anschrift:** | ClickHouse, Inc., 650 Castro St, Ste. 120 Unit 92426, Mountain View, California 94041, USA |

| | |
|---|---|
| **Beschreibung der Verarbeitung:** | Einsatz als analytische Datenbank zur Speicherung der im Rahmen des Varify Realtime Tracking erhobenen Event-Daten. Die Auswertung der Testergebnisse erfolgt in der Varify-Anwendung, nicht bei ClickHouse. Der Dienst ist optional und wird ausschließlich eingesetzt, wenn der Verantwortliche das Realtime Tracking in seinem Account freischaltet. |
| **Betroffene Datenkategorien:** | Anonymous-ID (UUID, beim Laden der Seite im Browser erzeugt, sofern noch nicht vorhanden, im localStorage abgelegt und über alle anonymen Events hinweg mitgeführt), Session-ID (im sessionStorage abgelegt, bei jedem neuen Tab und jeder neuen Sitzung neu erzeugt), User-Agent, Browser-Navigationsinformationen, aus dem User-Agent abgeleitete Geräteinformationen sowie die Zeitzone des Browsers. Weitere Daten werden nicht übermittelt. IP-Adressen werden nicht an ClickHouse übermittelt und dort folglich nicht verarbeitet. Die Übermittlung personenbezogener Daten in Event-Properties ist nicht zugelassen. Auf der Website des Verantwortlichen wird kein ClickHouse-Tracker geladen; es besteht keine direkte Verbindung zwischen dem Endgerät des Betroffenen und ClickHouse. |
| **Ort der Verarbeitung:** | ClickHouse Cloud Region eu-central-1, Frankfurt am Main, Deutschland |
| **Datenschutzrechtliches Vertragsverhältnis:** | Es gilt das ClickHouse Customer Data Processing Addendum. Die Standardvertragsklauseln sind darin durch Verweisung aufgenommen; Modul 3 (Auftragsverarbeiter an Auftragsverarbeiter) findet Anwendung, soweit der Auftragsverarbeiter selbst als Auftragsverarbeiter handelt. Ergänzend besteht ein Angemessenheitsbeschluss (das Data Privacy Framework) und der Anbieter ist entsprechend zertifiziert. Die Speicherung erfolgt ausschließlich in der EU. |