Vertrag über die Auftragsdatenverarbeitung

zwischen

.....

.....

.....

– **Verantwortlicher**, nachstehend „**Auftraggeber**“ genannt –

und

steep GmbH

Justus-von-Liebig-Straße 18

53121 Bonn

– **Auftragsverarbeiter**, nachstehend „**Auftragnehmer**“ genannt –

– Zusammen die **„Parteien“** –

1. Gegenstand und Dauer des Vertrags

1) Der Gegenstand des Vertrags ergibt sich aus dem Vertrag über die Bereitstellung des Meldeportals Whistleblowingportal.com vom ....., auf die hier verwiesen wird (nachstehend „Hauptvertrag“).

2) Dieser Vertrag sichert die rechtmäßige Verarbeitung personenbezogener Daten des Auftraggebers durch den Auftragnehmer. Sofern Regelungen des Datenschutzes oder dieses Vertrages dem Schutzzweck der Whistleblower-Richtlinie (EU) Nr. 2019/1937 beziehungsweise der nationalen Umsetzung widersprechen, gehen der Schutz des Hinweisgebers und die rechtskonforme Anwendung der Richtlinie (EU) Nr. 2019/1937 sowie der nationalen Umsetzung vor.

3) Die Dauer dieses Vertrags (Laufzeit) entspricht der Laufzeit des Hauptvertrags.

4) Der Vertrag gilt unbeschadet des vorstehenden Absatzes so lange, wie der Auftragnehmer personenbezogene Daten des Auftraggebers verarbeitet (einschließlich Backups).

5) Soweit sich aus anderen Vereinbarungen zwischen Auftraggeber und Auftragnehmer anderweitige Abreden zum Schutz personenbezogener Daten ergeben, soll dieser Vertrag zur Auftragsverarbeitung vorrangig gelten, es sei denn, die Parteien vereinbaren ausdrücklich eine andere Regelung.

2. Konkretisierung der Datenverarbeitung

1) Art der Daten

Der Gegenstand der Verarbeitung personenbezogener Daten bemisst sich im Wesentlichen nach der durch den Hauptvertrag festgelegten Verwendung durch den Auftraggeber beziehungsweise die Hinweisgeber. Personenbezogene Daten, die möglicherweise durch den Auftragnehmer verarbeitet werden, sind diejenigen Daten, die der Hinweisgeber selbst in das System einpflegt, wie:

- ☒ Personenstammdaten
- ☒ Kommunikationsdaten (z.B. Telefon, E-Mail, aber auch Kommunikationsinhalt)
- ☒ Vertragsstammdaten
- ☒ Kundenhistorie
- ☒ Vertragsabrechnungs- und Zahlungsdaten
- ☒ Planungs- und Steuerungsdaten

☒ Auskunftsangaben (von Dritten, z.B. Auskunfteien oder aus öffentlichen Verzeichnissen)

☒ Weitere personenbezogene Daten, welche durch den Hinweisgeber offengelegt werden

2) Zweck der vorgesehenen Verarbeitung von Daten

Der Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer ist die Erfüllung der im Hauptvertrag beschriebenen Tätigkeit.

3) Kategorien betroffener Personen

Die Kategorien der durch die Datenverarbeitung betroffenen Personen umfassen:

☒ Kunden

☒ Interessenten

☒ Abonnenten

☒ Lieferanten

☒ Handelsvertreter

☒ Ansprechpartner

☒ Beschäftigte

☒ Management, Geschäftsführung

☒ Personen aus (Kontroll-)Gremien

☒ Weitere betroffene Personen, welche sich aus der Kommunikation mit dem Hinweisgeber ergeben

3. Technisch-organisatorische Maßnahmen

1) Der Auftragnehmer ergreift in seinem Verantwortungsbereich alle erforderlichen technisch-organisatorische Maßnahmen gemäß Art. 32 DS-GVO zum Schutz der personenbezogenen Daten und übergibt dem Auftraggeber die Dokumentation zur Prüfung **(Anlage B.1)**. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Bestandteil des Vertrags.

2) Soweit die Prüfung / ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, soll versucht werden, diesen einvernehmlich umzusetzen.

3) Die vereinbarten technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem

Auftragnehmer gestattet, zukünftig alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Über wesentliche Änderungen, die durch den Auftragnehmer zu dokumentieren sind, ist der Auftraggeber zeitnah in Kenntnis zu setzen.

4. Berichtigung, Einschränkung und Löschung von Daten

1) Der Auftragnehmer unterstützt den Auftraggeber in seinem Verantwortungsbereich und soweit möglich mittels geeigneter technisch-organisatorischer Maßnahmen bei der Beantwortung und Umsetzung von Anträgen betroffener Personen hinsichtlich ihrer Datenschutzrechte. Er darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers beauskunften, portieren, 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) Soweit vom Leistungsumfang umfasst, sind die Rechte auf Auskunft, Berichtigung, Einschränkung der Verarbeitung, Löschung sowie Datenportabilität nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

3) Absätze 1) und 2) finden keine Anwendung, sofern ihre Durchführung dem Sinn und Zweck des Hinweisgeberschutzes widersprechen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat, zusätzlich zu der Einhaltung der Regelungen dieses Vertrags, eigene gesetzliche Pflichten gemäß der DS-GVO; insofern gewährleistet er insbesondere die Einhaltung der hier folgenden Vorgaben.

1) Die Wahrung der Vertraulichkeit gemäß Art. 28 III lit. b), 29, 32 IV DS-GVO: 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. Die Verpflichtung zur Vertraulichkeit gilt auch nach Beendigung der Leistungsvereinbarung und dieser Vereinbarung. Der Auftragnehmer und alle dem Auftragnehmer unterstellten Personen 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 unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Vertrag beziehen: 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. Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

3) Unterstützung des Auftraggebers bei Anfragen durch die Aufsichtsbehörden: Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten, einem anderen Anspruch oder einem Informationsersuchen im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

4) Selbstkontrolle des Auftragnehmers: 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.

5) Meldung von Datenschutzverletzungen: Der Auftragnehmer meldet Verletzungen des Schutzes personenbezogener Daten unverzüglich an den Auftraggeber in der Weise, dass der Auftraggeber seinen gesetzlichen Pflichten nachkommen kann, insbesondere jenen nach Art. 33, 34 DS-GVO. Er fertigt über den gesamten Vorgang eine Dokumentation an, die er dem Auftraggeber für weitere Maßnahmen auf Anfrage zur Verfügung stellt.

6) Unterstützung bei Datenschutz-Folgenabschätzungen: Soweit der Auftraggeber zur Durchführung einer Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO verpflichtet ist, unterstützt ihn der Auftragnehmer unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen. Gleiches gilt für eine etwaig bestehende Pflicht zur Konsultation der zuständigen Datenschutz-Aufsichtsbehörde.

6. Unterauftragsverhältnisse

1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer in Anspruch nimmt, z.B. Telekommunikationsleistungen, Post- / Transportdienstleistungen, Reinigungsleistungen oder Bewachungsdienstleistungen. Wartungs- und

Prüfleistungen stellen dann ein Unterauftragsverhältnis dar, wenn sie für IT-Systeme erbracht werden, die im Zusammenhang mit einer Leistung des Auftragnehmers nach diesem Vertrag erbracht werden. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

2) Der Auftraggeber stimmt der Beauftragung der in **Anlage B.2** bezeichneten Unterauftragnehmer unter der Bedingung einer vertraglichen Vereinbarung mit dem Unterauftragnehmer nach Maßgabe des Art. 28 II – IV DS-GVO zu.

3) Die Auslagerung auf Unterauftragnehmer oder der Wechsel der gemäß **Anlage B.2** bestehenden Unterauftragnehmers sind zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber in einer angemessenen Zeit, die 14 Tage nicht unterschreiten darf, vorab schriftlich oder in Textform anzeigt und
- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 II – IV DS-GVO zugrunde gelegt wird.

4) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

5) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU / des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher.

6) Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

7. Internationale Datentransfers

1) Jede Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation bedarf einer dokumentierten Weisung des Auftraggebers und bedarf der Einhaltung der Vorgaben zur Übermittlung personenbezogener Daten in Drittländer nach Kapitel V der DS-GVO.

2) Soweit der Auftraggeber eine Datenübermittlung in ein Drittland anweist, ist er für die Einhaltung von Kapitel V der DS-GVO verantwortlich.

8. 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 rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb während der üblichen Geschäftszeiten zu überzeugen.

2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO 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.

3) Der Nachweis der technisch-organisatorischen Maßnahmen zur Einhaltung der besonderen Anforderungen des Datenschutzes allgemein sowie solche, die den Auftrag betreffen, kann erfolgen durch

- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen angemessenen Vergütungsanspruch geltend machen.

9. Weisungsbefugnis des Auftraggebers

1) Der Auftragnehmer verarbeitet personenbezogene Daten nur auf Basis der im Hauptvertrag charakterisierten Weisungen des Auftraggebers, es sei denn er ist nach dem Recht des Mitgliedstaats oder nach Unionsrecht zu einer Verarbeitung verpflichtet. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform). Der Auftragnehmer hat das Recht, Weisungen, die dem Sinn und Zweck des Hinweisgeberschutzes widersprechen, nicht auszuführen. Er teilt dem Auftraggeber diese Entscheidung und die hierzu führenden Argumente mit.

2) 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 bestätigt oder geändert wird.

10. Rückgabe und Löschung personenbezogener Daten

1) Nach Beendigung des Vertrages hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, zu löschen. Etwaige gesetzliche Aufbewahrungspflichten oder sonstige Pflichten zur Speicherung der Daten bleiben unberührt. Für Datenträger gilt, dass diese im Falle einer vom Auftraggeber gewünschten Löschung sicherheitskonform zu vernichten sind.

2) Der Auftragnehmer darf personenbezogene Daten, die im Zusammenhang mit dem Auftrag verarbeitet worden sind, über die Beendigung des Vertrages hinaus speichern, wenn und soweit den Auftragnehmer eine gesetzliche Pflicht zur Aufbewahrung trifft. In diesen Fällen dürfen die Daten nur für Zwecke der Umsetzung der jeweiligen gesetzlichen Aufbewahrungspflichten verarbeitet werden. Nach Ablauf der Aufbewahrungspflicht sind die Daten unverzüglich zu löschen.

3) Absatz 1) findet keine Anwendung, sofern die Durchführung dem Sinn und Zweck des Hinweisgeberschutzes widerspricht.

11. Datenschutzbeauftragte

1) Der Auftraggeber bestätigt, bei Vorliegen der gesetzlichen Notwendigkeit, dass er einen Datenschutzbeauftragten nach Art. 37 DS-GVO benannt hat. Der Auftraggeber trägt Sorge dafür, dass der Datenschutzbeauftragte über die erforderliche Qualifikation und das erforderliche Fachwissen verfügt.

2) Der Auftragnehmer bestätigt, dass er einen Datenschutzbeauftragten nach Art. 37 DS-GVO benannt hat. Der Auftragnehmer trägt Sorge dafür, dass der Datenschutzbeauftragte über die erforderliche Qualifikation und das erforderliche Fachwissen verfügt. Der Datenschutzbeauftragte ist unter Datenschutz@steep.de jederzeit zu erreichen.

12. Benachrichtigungspflichten, Haftung, Schriftform, Verhältnis zum Hauptvertrag, salvatorische Klausel, Rechtswahl und Gerichtsstand

1) In dem Fall, dass die personenbezogenen Daten Gegenstand einer Durchsuchung, Pfändung oder Beschlagnahme während einer Insolvenz oder aus anderem Anlass oder aufgrund der Maßnahmen Dritter werden, während sie sich im Verfügungsbereich des Dienstleisters befinden, ist der Dienstleister verpflichtet, den Auftraggeber unverzüglich zu informieren. Der Dienstleister ist ferner verpflichtet, alle befugten Personen in diesen Verfahren darüber zu informieren, dass es sich bei

den betroffenen personenbezogenen Daten um Daten des Auftraggebers handelt, für die der Auftraggeber der Verantwortliche ist.

2) Hinsichtlich der Haftung wird auf Art. 82 DS-GVO verwiesen.

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

4) Diese Vereinbarung regelt die Mindestanforderungen an die Verarbeitung personenbezogener Daten durch den Auftragnehmer im Auftrag des Auftraggebers. Insoweit gehen im Fall abweichender Regelungen die Regelungen dieser Vereinbarung den Regelungen des Hauptvertrags vor. Strengere Pflichten für den Dienstleister in Bezug auf die Verarbeitung personenbezogener Daten aus dem Hauptvertrag lässt sie unberührt.

5) Für den Fall, dass einzelne Regelungen dieser Vereinbarung ganz oder teilweise unwirksam oder undurchführbar sind oder werden, oder für den Fall, dass diese Vereinbarung unbeabsichtigte Lücken enthält, wird dadurch nicht die Wirksamkeit der übrigen Regelungen berührt. Anstelle der unwirksamen, undurchführbaren oder fehlenden Regelung werden die Parteien eine solche wirksame und durchführbare Regelung vereinbaren, wie sie die Parteien unter Berücksichtigung des wirtschaftlichen Zwecks dieser Vereinbarung vereinbart hätten, wenn ihnen beim Abschluss dieser Vereinbarung die Unwirksamkeit, Undurchführbarkeit oder das Fehlen der betreffenden Regelung bewusst gewesen wäre.

6) Rechtsstreitigkeiten in Zusammenhang mit Vereinbarung unterliegen dem Recht der Bundesrepublik Deutschland. Gerichtsstandort ist Bonn.

Anlage B.1 – Technisch-organisatorische Maßnahmen

Diese können dem beigefügten Dokument „**Anlage B.1 TOMs**“ entnommen werden, welches Bestandteil dieser Vereinbarung wird.

Anlage B.2 – Genehmigte Unterauftragsverhältnisse

Firma Unterauftragnehmer	Anschrift Land	Leistung	Angaben zu geeigneten Garantien bei Übermittlungen in ein Drittland
Hetzner **Online GmbH**	Industriestraße 25 91710 Gunzenhausen Deutschland	Cloud Services	Keine Datenübermittlung in ein Drittland