Vertrag über die Auftragsverarbeitung

nach Art. 28 Abs. 3 DSGVO

zwischen der

shipzero GmbH
St. Annenufer 2,
DE-20457 Hamburg

(im Folgenden „Auftragnehmer“)

und dem „Auftraggeber“, der durch die Annahme dieses Vertrags den Bedingungen zustimmt

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand

Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer: Erstellung von (teil-) automatisierten und Datenquellen-übergreifenden Reportings zum Zwecke der Transportemissions-Auswertung. Dies umfasst konkret die Auswertung von transportrelevante Kennzahlen bzw. Attributinformationen, sowie technische Fahrzeugdaten aus Telematiksystemen externer Transportpartner. Resultierende Reports werden für spezifische Stakeholder auf Basis eines Berichtigungskonzeptes über eine Web-Oberfläche zur Verfügung gestellt.

(2) Dauer

Die Verarbeitung wird auf unbestimmte Zeit geschlossen und erlischt nach Abschluss der Zusammenarbeit. Die Zusammenarbeit wird vom Auftraggeber eigenständig verwaltet. Der Auftraggeber kann die Zusammenarbeit zudem jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DS-GVO

Convenience Translation

Data processing agreement

According to Art. 28 Par. 3 GDPR

Between the “Assigned Company”

shipzero GmbH
St. Annenufer 2,
20457 Hamburg
Germany

and the “Contracting Company”, who agrees to the terms and conditions by accepting this contract

1. Subject and duration of the contract

(1) Subject

The subject of the contract for handling and processing data is the performance of the following tasks by the Assigned Company: Creation of (partially) automated and cross-data source reporting for the purpose of transport emission evaluation. Specifically, this includes the evaluation of transport-relevant key figures and attribute information, as well as technical vehicle data from telematics systems of external transport partners. Resulting reports are made available to specific stakeholders on the basis of an access rights concept via a web interface.

(2) Duration

The processing shall be concluded for an indefinite period and shall expire after completion of the cooperation. The Contracting Company may terminate the cooperation at any time without notice, if there is a serious breach of data protection regulations or of the provisions of this contract by the Assigned Company; the Assigned Company cannot or will not carry out an instruction of the Contracting Company or the Assigned Company refuses control rights of the Contracting Company that are in breach of the contract.

In particular, non-compliance with the obligations agreed in this contract and derived from Art. 28 GDPR constitutes a serious breach.

abgeleiteten Pflichten stellt einen schweren Verstoß dar.

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Die Verarbeitung ist folgender Art: Es werden automatisiert Daten aus unterschiedlichen Datenquellen ausgelesen, organisiert, gespeichert und aufbereitet.

Die Verarbeitung dient folgendem Zweck: Es sollen Datenanalysen zur freiwilligen und regulatorisch oder vertraglich verpflichtenden Ausweisung von Treibhausgasemissionen aus Transportaktivitäten bereitgestellt werden. Dies umfasst auch die Identifikation wirtschaftlicher und ökologischer Optimierungspotenziale. Dazu soll ein Reporting-System für vorab definierte Empfängerkreise zur Einhaltung geltender Rechtsvorschriften und zur Optimierung der Unternehmenssteuerung eingeführt werden.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

(2) Art der Daten

Gegenstand der Verarbeitung sind transport- und auftragsrelevante Informationen zur Fracht, Fahrzeugstellung (Disposition), Fahrzeug-eigenschaften, Auftraggebern, Unterauftrag-nehmern, Versandbedingungen, Frachtführer, Auftraggeber sowie interne Organisations-merkmalen (Abteilungen, administrative Regionen, Sendungsarten).

Notwendige personenbezogene Daten werden ausschließlich für zugangsrelevante, nutzungs-berechtige Mitarbeiter gespeichert (Name, Abteilung, e-Mail).

Quellsysteme der Daten sind im Hinblick auf Telematikdaten web-basierte Datenschnittstellen der Hersteller oder vom Auftraggeber eingesetzte Drittsysteme, wie Tankkartensysteme. Für Auftrags- und Transportinformationen werden

2. Specification of the contract content

(1) Type and purpose of the intended processing of data

The processing is of the following type: Data from different data sources are read, organized, stored and prepared in an automated manner.

The processing serves the following purpose: Data analyses are to be provided for the voluntary and regulatory or contractually obligatory reporting of greenhouse gas emissions from transport activities. This also includes the identification of economic and ecological optimization potentials. To this end, a reporting system is to be introduced for predefined groups of recipients to ensure compliance with applicable legislation and to potentially optimize corporate strategies and management.

The provision of the contractually agreed data processing shall take place exclusively in a member state of the European Union or in another state party that is defined by agreement on the European Economic Area. Any relocation to a third country requires the prior consent of the client and may only take place if the special requirements of Art. 44 et seq. GDPR are fulfilled.

(2) Type of data

The object of processing are transport and order-relevant information on freight, cargo weight, product specification, vehicle position (dispatchment), vehicle characteristics, clients, subcontractors, and on internal organizational features (departments, administrative regions, shipment types).

Necessary personal data are stored exclusively for access-relevant, authorized employees (name, department, e-mail).

With regard to telematics data, the source systems of the data are web-based data interfaces of the manufacturers or third-party systems used by the customer, such as fuel card systems. With regard to order and transport information, the source systems of the data are transport management or ERP systems.

das Transport-Managementsystem, das ERP-System oder hiervon abstrahierte Informationen aus einem Data Warehouse oder Business Intelligence Tool verwendet.

Die Datenspeicherung und -verarbeitung zu Analysezwecken durch den Auftragnehmer erfolgt ausschließlich über zertifizierte Cloud-Anbieter, die eine Datenverarbeitung nach einem dem europäischen Datenschutz vergleichbaren Standard garantieren muss. Datenaustausch und Kommunikationswege zwischen Auftragnehmer, Auftraggeber und etwaigen Systemherstellern sind marktüblich verschlüsselt.

(3) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen: Beschäftigte, Beschäftigte von Dienstleistern.

3. Technisch-organisatorische Maßnahmen

(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 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO 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 DS-GVO zu berücksichtigen [Einzelheiten in Anlage 1].

Data storage and processing for analyzing purposes by the employee shall be carried out exclusively via certified cloud providers, which must guarantee data processing in accordance with a standard comparable to European data protection. Data exchange and communication paths between the Assigned Company, the Contracting Company and any system manufacturers are encrypted in accordance with standard market practices.

(3) Categories of affected persons

The categories of subjects affected by the processing include: Employees and employees of service providers.

3. Technical-organizational measures

(1) The Assigned Company shall document the implementation of the technical and organizational measures set out and required in the setup before the start of the processing, in particular with regard to the specific execution of the order, and shall hand them over to the Contracting Company for inspection. If accepted by the Contracting Company, the documented measures shall become the basis of the contract. Insofar as the inspection/audit of the Contracting Company reveals a need for adaptation, this shall be implemented by mutual agreement.

(2) The Assigned Company shall establish security according to Art. 28 Para. 3 lit. c, 32 GDPR, in particular in connection with Art. 5 Para. 1, Para. 2 GDPR. Overall, the measures to be taken are data security measures and to ensure a level of appropriate risk protection with regards to confidentiality, integrity, availability and the resilience of the systems. The state of the art, the implementation costs and the type, scope and purposes of the processing as well as the varying likelihood and severity of the risk to the rights and freedoms of natural persons within the meaning of Article 32 (1) of the GDPR must be taken into account [details in Appendix 1].

(3) The technical and organizational measures are subject to technical progress and further development. In this respect, the Assigned

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

(4) Der Auftraggeber stimmt zu, dass der Auftragnehmer entsprechend berechtigt ist, die aufgeführten Daten abzufragen und zu verarbeiten, insbesondere durch Integration des Telematik-Anbieters oder andere Formen der direkten Integration per API. Der Auftraggeber wird die hierfür benötigten Informationen (Dokumentationen, Zugänge) entsprechend bereitstellen. Allein der Auftraggeber ist für die Rechtmäßigkeit der bereitgestellten Informationen, Instruktionen sowie generell für die Bereitstellung der Daten verantwortlich.

4. Haftung gegenüber Dritten

(1) Der Auftraggeber erkennt an, dass der Auftragnehmer auf Drittsysteme zugreift (z.B. Telematikdaten), die von externen Partnern auf Basis von Zugangsdaten bereitgestellt werden, die vom Auftraggeber geteilt wurden. Der Auftraggeber stellt sicher, dass ein solcher Zugriff durch seine Vereinbarungen mit den Partnern autorisiert ist und dass die Verwendung der Zugangsdaten den geltenden Nutzungsbedingungen zwischen dem Auftraggeber, seinen Partnern und den Telematikanbietern entspricht.

(2) Der Auftragnehmer haftet nicht für Verstöße gegen die Nutzungsbedingungen oder Dienstleistungsvereinbarungen zwischen dem Auftraggeber (oder seinen Partnern) und den Drittanbietern, wenn solche Verstöße auf die Bereitstellung von Zugangsdaten oder den Zugang durch den Auftraggeber an den Auftragnehmer zurückzuführen sind. Der Auftraggeber trägt die volle Verantwortung dafür, dass diese Nutzungsbedingungen eingehalten werden.

(3) Keine der Parteien haftet für indirekte, zufällige, Folgeschäden oder Strafschadensersatz, einschließlich entgangenen Gewinns oder Umsatzes, die sich aus oder im Zusammenhang mit dieser Vereinbarung ergeben, es sei denn, sie wurden durch Vorsatz oder grobe Fahrlässigkeit verursacht.

Company is permitted to implement alternative adequate measures. In doing so, the security level of the specified measures must not be undercut. Significant changes shall be documented.

(4) The Contracting Company agrees that the Assigned Company is authorized to query and process the listed data, in particular by integrating the vehicle telematics systems or other forms of direct integration via API. The Contracting Company shall provide the information required for this (documentation, access). The Contracting Company alone is responsible for the legality of the information provided, instructions as well as generally for the provision of the data.

4. Third-party Liability

(1) The Contracting Company acknowledges that the Assigned Company may access third-party systems (e.g. telematics data) provided by external partners through login credentials shared by the Contracting Company. The Contracting Company shall ensure that such access is authorized by its agreements with the partners and that the use of login credentials complies with the relevant terms of service between the Contracting Company, its partners, and the telematics providers.

(2) The Assigned Company shall not be liable for any breach of the terms of use or service agreements between the Contracting Company (or its partners) and third parties if such breach arises from the Contracting Company providing login credentials or access to the Assigned Company. The Contracting Company shall bear full responsibility for ensuring compliance with these terms of service.

(3) Neither party shall be liable for indirect, incidental, consequential, or punitive damages, including lost profits or revenue, arising out of or in connection with this agreement, unless caused by willful misconduct or gross negligence.

5. 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) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

6. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

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

a) Der Auftragnehmer hat einen externen Datenschutzbeauftragten bestellt.
DataCo GmbH,
Nymphenburger Str. 86,
80636 München
Telefon: +49 89 8967 5514 30
E-Mail: datenschutz@dataguard.de
Als Ansprechpartner beim Auftragnehmer wird Herr Tobias Bohnhoff benannt.

b) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 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. 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.

5. Correction, restriction and deletion of data

(1) The Assigned Company may not correct, delete or restrict the processing of data that fall into the order scope on its own authority, but only in accordance with documented instructions from the Contracting Company. If an affected subject contacts the Assigned Company directly in this regard, the Assigned Company shall forward this request to the Contracting Company without delay.

(2) Insofar as included in the scope of services, the deletion concept, the right to be forgotten, correction, data portability and information shall be ensured directly by the Assigned Company in accordance with the Contracting Company's documented instructions.

6. Quality assurance and other obligations of the Assigned Company

In addition to compliance with the provisions of the order, the Assigned Company shall have statutory obligations according to Articles 28 to 33 of the GDPR; in this respect, the Assigned Company shall in particular ensure compliance with the following requirements:

a) The Assigned Company has appointed an external data protection officer. The data protection officer is represented by
DataCo GmbH,
Nymphenburger Str. 86,
80636 Munich
Phone: +49 89 8967 5514 30
E-Mail: datenschutz@dataguard.de
Mr. Tobias Bohnhoff (tobias@shipzero.com) servers as internal contact person for the Assigned Company.

b) The maintenance of confidentiality shall be in accordance to Art. 28 (3) sentence 2 lit. b, 29, 32 (4) GDPR. When carrying out the work for the actual order, the Assigned Company shall only use employees who have been obligated to maintain confidentiality and who have been familiarized in advance with the data protection provisions relevant to them. The Assigned Company and any person subordinate to the Assigned Company who has access to personal data may process such data solely in accordance with the Contracting Company's instructions, including the authorizations

c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten in Anlage 1].

d) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

e) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag 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.

f) 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.

g) 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.

h) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

granted in this agreement, unless they are required by law to process it.

c) The implementation of and compliance with all technical and organizational measures required for this order shall be in accordance with Art. 28 (3) p. 2 lit. c, 32 GDPR [details in Annex 1].

d) The Contracting Company and the Assigned Company shall, upon request, cooperate with the supervisory authority in the performance of its duties.

e) The immediate information of the Contracting Company about control actions and measures of the supervisory authority, insofar as they relate to this order. This shall also apply insofar as a competent authority investigates in the context of administrative offense or criminal proceedings with regard to the processing of personal data during the commissioned processing at the Assigned Company.

f) Insofar as the Contracting Company is exposed on its part to an inspection by the supervisory authority, administrative offense or criminal proceedings, the liability claim of a data subject or to a third party or any other claim in connection with the commissioned processing at the Assigned Company, the Assigned Company shall support the Contracting Company to the best of its ability.

g) The Assigned Company shall regularly monitor the internal processes as well as the technical and organizational measures to ensure that the processing in his area of responsibility is carried out in accordance with the requirements of the applicable data protection law and that the protection of the rights of the affected subjects is guaranteed.

h) Verifiability of the technical and organizational measures to the Contracting Company, within the scope of its control authorizations, according to Section 7 of this Agreement.

7. 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 z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. 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 sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen [Auflistung der Unterauftragsverhältnisse in Anlage 2].

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

(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen (z.B. Einwilligungserklärung des Auftraggebers oder vollständige Anonymisierung der verarbeiteten Informationen) sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

(5) Eine weitere Auslagerung durch den Unterauftragnehmer ist nicht gestattet.

7. Subcontract relationships

(1) Subcontracting relationships within the meaning of this contract shall be understood to be those services which relate directly to the provision of the main service. This does not include ancillary services which the Assigned Company uses, for example, as telecommunications services, postal/transport services, maintenance and user service or the disposal of data media and other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing systems. However, the Assigned Company shall be obligated to enter into appropriate and legally compliant contractual agreements as well as control measures to ensure data protection and data security of the Contracting Company's data even in the case of outsourced ancillary services.

(2) The Assigned Company may engage subcontractors (further processors) only with the prior, explicit written or documented consent of the Contracting Company [list of subcontracting relationships in Annex 2].

(3) The transfer of personal data of the Contracting Company to the subcontractor (of the Assigned Company) and its first activity shall be permitted only after all requirements for subcontracting have been met.

(4) If the subcontractor provides the agreed service outside the EU/EEA, the Assigned Company shall ensure admissibility under data protection law by taking appropriate measures (e.g. declaration of consent by the Contracting Company or complete anonymization of the processed information). The same applies if service providers within the meaning of Paragraph 1 Sentence 2 are to be used.

(5) Further outsourcing by the subcontractor is not permitted.

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 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 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 solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren).

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

8. Control rights of the Contracting Company

(1) The Contracting Company has the right to carry out inspections in consultation with the Assigned Company or to have them carried out by inspectors that are to be named in the respective cases. The Contracting Company has the right to approve the Assigned Company's compliance with this agreement in its business operations by means of spot checks, which must generally be notified in time.

(2) The Assigned Company shall ensure that the Contracting Company can approve the Assigned Company's compliance with its obligations according to Art. 28 of the GDPR The Assigned Company agrees to provide the Contracting Company with the necessary information upon request and, in particular, to provide evidence of the implementation of the technical and organizational measures.

(3) Evidence of such measures, which do not only relate to the specific order, can be provided in the form of current test certificates, reports or report extracts from independent bodies (e.g. auditors, auditing, data protection officers, IT security department, data protection auditors, quality auditors).

(4) The Assigned Company may claim remuneration for enabling inspections by the Contracting Company.

9. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO 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, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich bereitzustellen
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 Vergütung beanspruchen.

10. Weisungsbefugnis des Auftraggebers

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

(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 so lange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird

9. Notification in case of violations by the contractor

(1) The Assigned Company shall support the Contracting Company in complying with the obligations set out in Articles 32 to 36 of the DSGVO regarding the security of personal data, data breach notification obligations, data protection impact assessments and prior consultations. This includes, among other things:

a) ensuring an adequate level of protection through technical and organizational measures that take into account the circumstances and purposes of the processing as well as the predicted likelihood and severity of a possible security breach and allow for the immediate detection of relevant breach events
b) the obligation to report personal data breaches to the Contracting Company without undue delay
c) the obligation to assist the Contracting Company within the scope of its duty to inform the affected subject and to provide it with all relevant information in this context without delay
d) the support of the Contracting Company for its data protection impact assessment
e) the support of the Contracting Company in the scope of prior consultations with the supervisory authority

(2) The Assigned Company may claim compensation for support services that are not included in the performance description, or that are not necessary due to his misconduct.

10. Authority of the Contracting Company to issue instructions

(1) The Contracting Company shall confirm verbal instructions without delay (at least in text form).

(2) The Assigned Company shall inform the Contracting Company immediately if he has the opinion that an instruction violates data protection regulations. The Assigned Company shall be entitled to suspend the execution of the relevant instruction until it is confirmed or adapted by the Contracting Company.

11. 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 vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

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

12. Verschiedenes

(1) Für alle Bestimmungen, die in diesem Vertrag nicht geregelt sind, gelten die Bestimmungen der Allgemeinen Geschäftsbedingungen von shipzero.

(2) shipzero behält sich das Recht vor, diese Datenverarbeitungsvertrag zu ändern. Jede Änderung erfordert die Zustimmung des Auftraggebers.

11. Deletion and return of personal data

(1) Copies or duplicates of the data will not be made without the knowledge of the Contracting Company. Excluded from this are security copies, insofar as they are necessary to ensure proper data processing, as well as data that is required in order to comply with statutory retention obligations.

(2) After completion of the contractually agreed work or earlier upon request by the Contracting Company - at the latest upon termination of the service agreement - the Assigned Company shall hand over to the Contracting Company all documents, processing and utilization results created and data files related to the contractual relationship that have come into his possession or, after prior consent, destroy them in accordance with data protection requirements. The same shall apply to testing and rejected material. The protocol of the deletion shall be submitted upon request.

(3) Documentation that serves as proof of orderly and proper data processing shall be kept by the Assigned Company beyond the end of the contract in accordance with the respective safekeeping periods. The Assigned Company may hand them over to the Contracting Company at the end of the contract to his own relief.

12. Miscellaneous

(1) For all provisions not governed by this agreement, the provisions of shipzero' general terms and conditions shall apply.

(2) shipzero reserves the right to modify this data processing agreement. Any amendment requires the consent of the Contracting Company.

ANLAGE 1 – TECHNISCH-ORGANISATORISCHE MASSNAHMEN

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- **Zugangskontrolle** (vormals: Zutrittskontrolle) - Kein unbefugter Zutritt zu Datenverarbeitungsanlagen: Gewährleistet durch Magnet- oder Chipkarten am Arbeitsort sowie Verschlüsselung von Datenträgern

- **Zugriffskontrolle** – Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben: Gewährleistet durch Berechtigungskonzepte sowie die Protokollierung von Zugriffen auf Auswertungssystemen;

- **Trennungskontrolle** - Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden: Gewährleistet durch Mandantenfähigkeit der genutzten Datenbank- und Datenverarbeitungssysteme
- **Pseudonymisierung & Verschlüsselung** (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO) Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen: Gewährleistet durch die Arbeit mit technischen Schlüsseln (SIDs) bei der Datenverarbeitung.

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

- **Transport-, Übertragungs-, Datenträger- und Benutzerkontrolle** (vormals: Weitergabekontrolle) - Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport sowie Verhinderung der Nutzung automatisierter Verarbeitungssysteme und Gewährleistung der Überprüfung von Stellen, an denen Daten übermittelt oder zur Verfügung gestellt wurden oder werden können.

APPENDIX 1 – TECHNICAL, ORGANIZATIONAL MEASURES

1. Confidentiality (Art. 32 Par. 1 lit. b GDPR)

- **Access control I** - No unauthorized access to data processing systems: ensured by magnetic or chip cards at the place of work and encryption of data media

- **Access control II** – Ensuring that those authorized persons to use an automated processing system have access only to the personal data covered by their access authorization: Ensured by authorization concepts as well as documentation of access to evaluation systems;

- **Separation control** - Separate processing of data that were collected for different purposes: Ensured by multi-client capability of the database and data processing systems used.

- **Pseudonymization & Encryption** (Art. 32 Par. 1 lit. a GDPR; Art. 25 Par. 1 GDPR) The processing of personal data in such a way that the data can no longer be attributed to a specific person without recourse to additional information, provided that such additional information is kept separately and is subject to appropriate technical and organizational measures: Ensured by working with technical keys (SIDs) during the data processing.

2. Integrity (Art. 32 Par. 1 lit. b GDPR)

- **Transport-, transmission-, data medium and user control** (formerly: Transfer control) - No unauthorized reading, copying, modification, or removal during electronic transmission or transport, as well as preventing the use of automated processing systems and ensuring verification of locations where data has been or may be transmitted or made available. Ensured through the use of Virtual Private Networks (VPN) when accessing processing systems.

Gewährleistet durch die Nutzung von Virtual Private Networks (VPN) beim Zugriff auf die Verarbeitungssysteme.

- **Eingabekontrolle** - Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Gewährleistet durch Protokollierung auf Datenbank- und Datenverarbeitungsebene.

- **Input control** - Determining whether and by whom personal data has been entered into, modified or removed from data processing systems. Ensured by documentation on database level and data processing level

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)

- **Verfügbarkeitskontrolle und Wiederherstellbarkeit** – Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust: Gewährleistet durch automatische Backups der genutzten Daten-Infrastruktur sowie Firewall und Virenschutz.

3. Availability and resilience (Art. 32 Par. 1 lit. c GDPR)

- **Availability control and recoverability** - Protection against accidental or deliberate destruction or loss: ensured by automatic backups of the data infrastructure used as well as firewall and virus protection.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

- **Datenschutz-Management**
  - interne Verfahrensverzeichnisse werden regelmäßig geprüft und angepasst
  - Einbindung des Ansprechpartners für Datenschutz bei Änderungen der Verfahren
  - Sicherheitsmaßnahmen werden regelmäßig kontrolliert

- **Incident-Response-Management**
  - Alle Vorfälle die datenschutzrelevant sein könnten werden dem definierten Ansprechpartner umgehend gemeldet.
  - Festgelegte Meldewege bei Sicherheitsvorfällen (IT & Datenschutz) an Aufsichtsbehörde, Auftraggeber, betroffene Personen, Dienstleister.

- **Datenschutzfreundliche Voreinstellungen** (Art. 25 Abs. 2 DS-GVO)
  - Minimierung der Erfassung und Verarbeitung personenbezogener Daten
  - Transparenz bei der Verwendung personenbezogener Daten
  - Deaktivierung von Datenverarbeitungsfunktionen, die für den

4. Procedures for regular review, assessment and evaluation (Art. 32 Par. 1 lit. d GDPR Art. 25 Par. 1 GDPR)

- **Data protection management**
  - Internal procedure directories are regularly reviewed and adapted
  - Involvement of the contact person for data protection in the event of changes to procedures
  - Security measures are checked regularly

- **Incident-Response-Management**
  - All incidents that could be relevant to data protection are reported immediately to the defined contact person.
  - Defined reporting channels in case of security incidents (IT & data protection) to supervisory authority, Contracting Company, affected subjects, service providers.

- **Privacy-friendly default settings** (Art. 25 Par. 2 GDPR)
  - Minimization of the collection and processing of personal data
  - Transparency in the use of personal data
  - Deactivation of data processing functions that are not required for the originally intended purpose

beabsichtigten Zweck nicht benötigt werden
    - Authentifizierungsfunktion und Rollenkonzepte, um technisch sicherzustellen, dass nur die tatsächlich Berechtigten Personen Zugriff auf die gespeicherten Daten haben

- **Auftragskontrolle**
    - Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers
    - zentrale Erfassung vorhandener Dienstleister
    - Durchführung von Kontrollen durch den Auftragnehmer

- Authentication function and role concepts to ensure technically that only the persons actually authorized have access to the stored data

- **Order control**
    - No commissioned data processing within the meaning of Art. 28 GDPR without corresponding instructions from the Contracting Company
    - Central registration of existing service providers
    - Implementation of controls by the Assigned Company

ANLAGE 2 – UNTERAUFTRAGSVERHÄLTNISSE

Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO. Die Datenhaltung und Verarbeitung findet ausschließlich auf Servern der Region West Europa (EU-Standorte Frankfurt am Main oder Amsterdam, Stand Mai 2024) statt:

APPENDIX 2 – SUBCONTRACTING RELATIONSHIPS

The Contracting Company agrees to the commissioning of the following subcontractors subject to the condition of a contractual agreement in accordance with Art. 28 (2-4) GDPR. Data storage and processing shall take place exclusively on servers in the Western Europe region (EU locations Frankfurt am Main or Amsterdam, as of June 2022):

Company subcontractor	**Address/Country**	**Description**
Microsoft Deutschland GmbH	Walter-Gropius-Straße 5, 80807 München, Germany	Microsoft Cloud Services (Hosting, Datenbases, API management)