Vertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

zwischen dem Auftraggeber gemäß Hauptvertrag

und

Echometer GmbH, Regina-Protmann-Str. 38, 48159 Münster

als Auftragsverarbeiter (nachfolgend „Auftragnehmer“ genannt)

§ 1 Vertragsgegenstand und Laufzeit

(1) Der Auftragnehmer erbringt für den Auftraggeber Leistungen auf Grundlage des SaaS-Vertrages zur Nutzung von Echometer („Hauptvertrag“). Dabei erhält der Auftragnehmer Zugriff auf personenbezogene Daten des Auftraggebers und verarbeitet diese ausschließlich im Auftrag und nach Weisung des Auftraggebers. Zur Konkretisierung der beiderseitigen datenschutzrechtlichen Rechte und Pflichten schließen die Parteien den vorliegenden Vertrag. Die Regelungen des vorliegenden Vertrages gehen im Zweifel den Regelungen des Hauptvertrages vor, soweit es sich um datenschutzrechtliche Regelungen handelt.

(2) Die Laufzeit dieses Vertrages richtet sich nach der Dauer der Verarbeitung.

§ 2 Gegenstand und Dauer der Verarbeitung

(1) Der Gegenstand der Verarbeitung ist die Bereitstellung einer Software-Lösung, mit der der Auftraggeber einen kontinuierlichen Verbesserungsprozess initiiert und steuert. Dabei wird Feedback der Teams eingeholt und dieses dem Auftraggeber im Sinne der Mitarbeiter-, Team- und Unternehmensentwicklung in Online-Workshops und Online-Ergebnisberichten aufbereitet.

(2) Die Dauer der Verarbeitung richtet sich nach der Laufzeit des Hauptvertrages. Die Verarbeitung kann über die Laufzeit des Hauptvertrages hinaus bis zur Rückgabe und Löschung bzw. Vernichtung der personenbezogenen Daten des Auftraggebers andauern.

§ 3 Art und Zweck der Verarbeitung

(1) Art der Verarbeitung ist das Hosting und die Wartung von Software und den darin vom Auftraggeber oder seinen Mitarbeitern eingebrachten personenbezogenen Daten sowie ggf. damit im Zusammenhang stehende Entwicklungsleistungen.

(2) Zweck der Verarbeitung ist die Einholung von Mitarbeiterfeedback. Dieses wird dem Auftraggeber im Sinne der Mitarbeiter-, Team- und Unternehmensentwicklung in Online-Workshops und Online-Ergebnisberichten aufbereitet.

§ 4 Art der personenbezogenen Daten und Kategorien betroffener Personen

(1) Arten personenbezogener Daten:

- Namen
- E-Mail-Adressen
- Passwörter
- Feedbacks von Mitarbeitern
- Innerhalb des Tools hinterlassene Notizen der Mitarbeiter

(2) Kategorien betroffener Personen:

- Beschäftigte

§ 5 Weisungsrecht

(1) Der Auftragnehmer darf personenbezogene Daten nur auf Weisung des Auftraggebers verarbeiten; dies gilt insbesondere in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation. Wird der Auftragnehmer durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(2) Die Weisungen des Auftraggebers werden anfänglich durch diesen Vertrag und den Hauptvertrag festgelegt und können vom Auftraggeber danach in Schriftform oder in Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden. Alle erteilten Weisungen sind sowohl vom Auftraggeber als auch vom Auftragnehmer zu dokumentieren.

(3) Dem Auftraggeber obliegt die Beurteilung der Zulässigkeit der Datenverarbeitung. Ist der Auftragnehmer jedoch der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Bestimmungen verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Der Auftragnehmer darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.

§ 6 Verpflichtung zur Vertraulichkeit

Der Auftragnehmer wird alle Personen, die von ihm mit der Verarbeitung von personenbezogenen Daten betraut werden, zur Vertraulichkeit verpflichten (Art. 28 Abs. 3 lit. b DS-GVO).

§ 7 Sicherheitsmaßnahmen

Der Auftragnehmer trifft alle erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 32 DS-GVO zum angemessenen Schutz der personenbezogenen Daten des Auftraggebers, insbesondere mindestens die in Anlage 1 aufgeführten Maßnahmen der Organisationskontrolle, Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle und Trennungskontrolle. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Über wesentliche Änderung der Sicherheitsmaßnahmen hat der Auftragnehmer den Auftraggeber unverzüglich zu unterrichten.

§ 8 Subunternehmer

(1) Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung der in Anlage 2 genannten Subunternehmer durchgeführt. Der Auftragnehmer ist im Rahmen seiner vertraglichen Verpflichtungen zur Begründung von weiteren Unterauftragsverhältnissen mit Subunternehmern befugt. Er setzt den Auftraggeber hiervon unverzüglich in Kenntnis. Der Auftragnehmer ist verpflichtet, Subunternehmer sorgfältig nach deren Eignung und Zuverlässigkeit auszuwählen. Der Auftragnehmer hat bei der Einschaltung von Subunternehmern diese entsprechend den Regelungen dieses Vertrages zu verpflichten und dabei sicherzustellen, dass der Auftraggeber seine Rechte aus diesem Vertrag (insbesondere seine Kontrollrechte) auch direkt gegenüber den Subunternehmern wahrnehmen kann. Sofern eine Einbeziehung von Subunternehmern in einem Drittland erfolgen soll, hat der Auftragnehmer sicherzustellen, dass beim jeweiligen Subunternehmer ein angemessenes Datenschutzniveau gewährleistet ist (z. B. durch Abschluss einer Vereinbarung auf Basis der EU-Standarddatenschutzklauseln).

(2) Unterauftragsverhältnisse mit Subunternehmern im Sinne dieser Bestimmungen liegen nicht vor, wenn der Auftragnehmer 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 Auftragnehmer für den Auftraggeber erbringt und Bewachungsdienste.

§ 9 Unterstützungspflichten

(1) Der Auftragnehmer unterstützt den Auftraggeber angesichts der Art der Verarbeitung nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III der DS-GVO genannten Rechte der betroffenen Personen nachzukommen.

(2) Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der dem Auftragnehmer zur Verfügung stehenden Informationen bei der Einhaltung seiner Pflichten nach Art. 32 bis 36 DS-GVO.

§ 10 Rückgabe und Löschung bzw. Vernichtung

Der Auftragnehmer wird nach Beendigung des Hauptvertrages alle personenbezogenen Daten nach Wahl des Auftraggebers entweder löschen bzw. vernichten oder zurückgeben und die vorhandenen Kopien löschen bzw. vernichten, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

§ 11 Kontrollrechte

(1) Der Auftragnehmer stellt dem Auftraggeber auf Verlangen alle erforderlichen Informationen zum Nachweis der Einhaltung der Pflichten des Auftragnehmers nach diesem Vertrag und nach Art. 28 DS-GVO zur Verfügung.

(2) Der Auftragnehmer ermöglicht dem Auftraggeber hierzu auch Überprüfungen - einschließlich Inspektionen -, die vom Auftraggeber oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, und trägt zu diesen bei. Der Auftraggeber wird Überprüfungen nur im erforderlichen Umfang durchführen und die Betriebsabläufe des Auftragnehmers dabei nicht unverhältnismäßig stören.

Anlage 1: Technische und organisatorische Maßnahmen der Echometer GmbH

§ 1 Allgemeine Angaben

Verantwortlicher	Robin Roschlau, Geschäftsführer (CIO) der Echometer GmbH
Datum	01.02.2020
Erhebung durch	Robin Roschlau, Geschäftsführer (CIO) der Echometer GmbH
Art der Erhebung	☐ Ersterhebung x Aktualisierung

§ 2 Erhebung

(1) Organisationskontrolle

TOM	**Vorhanden?**	**Bemerkung**
Datenschutz-Management (Interne Richtlinien)	x	
Verpflichtung der Beschäftigten zur Vertraulichkeit	x	
Verpflichtung der Beschäftigten auf das Fernmeldegeheimnis	x	
Verpflichtung von externen Dienstleistern auf das Datengeheimnis, sofern es sich nicht um Auftragsverarbeiter handelt	x	
Benennung eines Ansprechpartners für den Datenschutz	x	Robin Roschlau, Geschäftsführer (CIO) der

		Echometer GmbH

(2) Zutrittskontrolle

Sicherungsmaßnahmen innerhalb des Gebäudes/der Geschäftsräume:

TOM	Vorhanden?	Bemerkung
Videoüberwachung	x	
Einbruchmeldeanlage/Alarmanlage	x	
Zentraler Empfangsbereich mit Personenkontrolle	x	
Besucherüberwachung (Elektronisches Besuchermanagementsystem, Besucherbuch, Begleitung durch Mitarbeiter etc.)	x	
Dokumentiertes Zutrittskontrollkonzept mit einer Festlegung und Dokumentation der berechtigten Personen	x	
Elektronisches Zutrittskontrollsystem für das Gebäude (Magnetstreifen/Speicherchip, RFID-Chip, Codeschloss, biometrisches Verfahren etc.)	x	
Schlüsseldokumentation	x	
Prozess zur Aufhebung nicht mehr benötigter Zutrittsrechte	x	

(3) Zugangskontrolle (Datenverarbeitungsanlagen auf Netz- und Serverebene)

TOM	Vorhanden?	Bemerkung
(Verschlüsselte) Identifikation und Authentifikation von Benutzern (User-ID und Passwort, Zweistufenauthentifizierung mit Magnet-/Chipkarte oder Token, biometrisches Verfahren etc.)	x	
Passwortregeln vorhanden (Mindestlänge, Zeichensatz, Gültigkeitsdauer, Ausschluss von Trivialkennworten etc.)	x	
Vorläufig vergebene Passwörter werden unverzüglich durch sichere Individualpasswörter ersetzt	x	
Sperre von Endgeräten beim Verlassen (Bildschirmsperre mit Passwortschutz automatisch nach Zeitablauf)	x	
Software-Firewall vorhanden	x	
Updates für Firewall werden regelmäßig automatisch installiert	x	
Anti-Virus-Software vorhanden, dessen Updates regelmäßig automatisch installiert werden	x	
Regelmäßiges automatisches Einspielen von Sicherheitspatches und/oder -updates bei Browsern	x	
Verschlüsselung von Datenträgern in mobilen Endgeräten	x	

Sichere Löschung von Datenträgern vor deren Wiederverwendung	x	
Verschlüsselung von mobilen Datenträgern	x	

(4) Zugriffskontrolle (Datenverarbeitungsanlagen)

TOM	Vorhanden?	Bemerkung
Rollenbasierte Berechtigungen wie Kategorien von Rollen und Rechte der Rollen, insbesondere nach „Lesen, Schreiben, Ausführen“	x	
Rollen- und Rechtekonzept mit einer Festlegung und Dokumentation der Rollen und Rechte der berechtigten Personen	x	
Prozess zur Aufhebung nicht mehr benötigter Rollen und Rechte	x	
Regelmäßige Überprüfung der Erforderlichkeit der vergebenen Rollen und Rechte	x	

(5) Weitergabekontrolle

TOM	Vorhanden?	Bemerkung
Regelmäßiges automatisches/manuelles Einspielen von Sicherheitspatches und/oder -updates bei E-Mail-Programmen	x	
Einsatz von E-Mail-Contentfiltern	x	

(6) Eingabekontrolle

TOM	Vorhanden?	Bemerkung
Protokollierung der Einrichtung und des Betriebes von IT-Systemen	☐	Nicht anwendbar, da keine eigenen IT-Systeme vorhanden
Protokollierung der Einrichtung/Änderung von Benutzern und Rechten (Dokumentation aller berechtigten Nutzer, Rechteprofile der berechtigten Nutzer, Dokumentation von Änderungen von Nutzern/Rechten, Dokumentation, wer die Benutzer und Rechte angeordnet/eingerichtet hat, Historie über die eingerichteten Nutzer und Rechte etc.)	x	Soweit durch verwendete Software unterstützt
Protokollierung von Systemänderungen (Dokumentation von funktionalen Systemänderungen/Erweiterungen einschließlich Testfälle, Testung, Testergebnisse und Freigabe, Dokumentation von Versionsänderungen oder Änderungen der technischen Umgebung des IT-Systems, Änderungen der Dateiorganisation oder des Dateiverwaltungssystems etc.)	☐	Nicht anwendbar, da keine eigenen IT-Systeme vorhanden
Protokollierung von Eingaben und Veränderungen (Datum und Uhrzeit von Zugriffen mit Kennung des Benutzers, Ausgeführte Aktionen, insbesondere Lösch- und Kopiervorgänge, Zugriff auf Dateien mit personenbezogenen oder vertraulichen personenbezogenen Inhalten, unbefugte und abgewiesene Zugriffsversuche, wiederholte Eingabe von fehlerhaften Passwörtern zu einem Login,	x	Soweit durch verwendete Software unterstützt

unbefugtes Einloggen und Überschreiten von Befugnissen, Benutzung von Admin-Accounts, Warnungen über unbefugtes Eindringen etc.)		

(7) Auftragskontrolle

Allgemein:

TOM	Vorhanden?	Bemerkung
Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich des Datenschutzes)	x	
Vorherige Prüfung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen	x	
Abschluss eines Vertrages oder eines anderen Rechtsinstruments nach Art. 28 DSGVO und Einhaltung dieser Regularien	x	
Vertraglich festgelegte Verantwortlichkeiten	x	

(8) Verfügbarkeitskontrolle

TOM	Vorhanden?	Bemerkung
Backup-Konzept	x	
Regelmäßige automatisierte Datensicherungen	x	
Sichere Übertragung von Datensicherungen	x	

Regelmäßige Überprüfung der Sicherungsdaten auf Vollständigkeit und Lesbarkeit	x	
Recovery-Konzept	x	
Prüfung der Rekonstruierbarkeit der Datenbestände durch regelmäßige Tests	x	
Administratorenpasswort/Notfallpassworte sicher hinterlegt	x	
Vier-Augen-Prinzip bei sensiblen Administratortätigkeiten	x	
Test- oder Entwicklungsumgebung vorhanden	x	

(9) Trennungskontrolle

TOM	**Vorhanden?**	**Bemerkung**
Logische Trennung von verschiedenen speichernden Stellen (Unternehmen)	x	
Trennung von Test- und Produktionsdaten	x	

§ 3 Abschluss

Bemerkungen	Die Beurteilung basiert auf den aktuell genutzten Büroräumen in der Founders Foundation in Bielefeld. Die Technischen und Organisatorischen Maßnahmen von DigitalOcean als Hosting-Dienstleister sind diesen TOMs angehängt.

Nächste Aktualisierung	Die Erhebung von technischen und organisatorischen Maßnahmen wird jährlich aktualisiert. Die nächste Aktualisierung findet dementsprechend bis zum 01.02.2021 statt.

Technische und organisatorische Maßnahmen der DigitalOcean, LLC.

The Security Measures applicable to the Services are as follows

Access Control

Unauthorized persons shall be prevented from gaining physical access to premises, buildings or rooms, where data processing systems are located which process personal data. Exceptions may be granted for the purpose of auditing the facilities to third party auditors as long as they are supervised by DigitalOcean and do not get access to the personal data themselves.

DigitalOcean has (without limitation) implemented the following controls:

Access Control
Controls to specify authorized individuals permitted to access personal data
Implemented an access control process to avoid unauthorized access to DigitalOcean's premises
Implemented an access control process to restrict access to data centres / rooms were data servers are located
Utilizes video surveillance and alarm devices with reference to access areas
Ensured that personnel without access authorization (e.g. technicians, cleaning personnel) are accompanied all times when access data processing areas

System Access Control

Data processing systems must be prevented from being used without authorization.

DigitalOcean has (without limitation) implemented the following controls:

System Access Control
Ensured that all systems processing personal data (this includes remote access) are password protected after boot sequences when left even for a short period to prevent unauthorized persons from accessing any personal data
Provides dedicated user IDs for authentication against systems user management for every individual
Assigns individual user passwords for authentication
Ensured that access control is supported by an authentication system

1

System Access Control
Controls to grant access only to authorized personnel and to assign only the minimum permissions necessary for those personal to access personal data in the performance of their function
Implemented a password policy that prohibits the sharing of passwords, outlines processes after a disclosure of a password
Ensured that passwords are always stored in encrypted form
Implemented a proper procedure to deactivate user account, when a user leaves the DigitalOcean or function
Implemented a proper process to adjust administrator permissions, when an administrator leaves DigitalOcean or function
Implemented a solution to log privileged access to critical systems

Data Access Control

Persons entitled to use a data processing system shall gain access only to the data to which they have a right of access, and personal data must not be read, copied, modified or removed without authorization in the course of processing.

DigitalOcean has (without limitation) implemented the following controls:

Data Access Control
Restricted access to files and programs based on a "need-to-know-basis"
Stored physical media containing personal data in secured areas
Controls to prevent use/installation of unauthorized hardware and/or software
Established rules for the safe and permanent destruction of data that are no longer required
Controls to grant access only to authorized personnel and to assign only the minimum permissions necessary for those personal to access personal data in the performance of their function

Data Transmission Control

Personal data must not be read, copied, modified or removed without authorization during transfer or storage and it shall be possible to establish to whom personal data was transferred.

DigitalOcean has (without limitation) implemented the following controls:

Data Transmission Control
Encrypt data during any transmission

Data Entry Control

DigitalOcean shall be able retrospectively to examine and establish whether and by whom personal data have been entered into data processing systems, modified or removed.

DigitalOcean has (without limitation) implemented the following controls:

Data Entry Control
Controls to log administrators' and users' activities
Controls to permit only authorized personnel to modify any personal data within the scope of their function

Job Control

Personal data being processed in the performance of a service for the DigitalOcean shall be processed solely in accordance with the services agreement in place between the DigitalOcean and DigitalOcean and in accordance with the instructions of the DigitalOcean.

DigitalOcean has (without limitation) implemented the following controls:

Job Control
Established controls to ensure processing of personal data only for contractual performance
Controls to ensure staff members and contractors comply with written instructions or contracts
Ensured that data is always physically or logically separated so that, in each step of the processing, the client from whom personal data originates can be identified.

Availability Control

Personal data shall be protected against disclosure, accidental or unauthorized destruction or loss.

DigitalOcean has (without limitation) implemented the following controls:

Availability Control
Arrangements to create back-up copies stored in specially protected environments
Contingency plans or business recovery strategies
Controls to ensure that personal data is not used for any purpose other than for the purposes it has been contracted to perform
Controls to prevent removal of personal data from DigitalOcean's business computers or premises for any reason (unless DigitalOcean has specifically authorized such removal for business purposes).

Implemented a process for secure disposal of documents or data carriers containing personal data
Implemented network firewalls to prevent unauthorized access to systems and services

Organizational Requirements

The internal organization of DigitalOcean shall meet the specific requirements of data protection. In particular, DigitalOcean shall take technical and organizational measures to avoid the accidental mixing of personal data.

DigitalOcean has (without limitation) implemented the following controls:

Organizational Requirements
Designated a data protection officer (or a responsible person if a data protection officer is not required by law)
Obtained the written commitment of the employees to maintain confidentiality
Trained staff on data privacy and data security
Implemented a formal security incident response process that is consistently followed for the management of security incidents
Trained staff in the security incident responder roles on the security incident process

Anlage 2: Subunternehmer

DigitalOcean, LLC. 101 Avenue of the Americas 10th Floor New York 10013 USA Telefon: +1 888 890 6714 Mail: privacy@digitalocean.com Die DigitalOcean, LLC. hat sich dem EU-US-PrivacyShield unterworfen. Ein aktuelles Zertifikat kann unter folgendem Link eingesehen werden. https://www.privacyshield.gov/participant?id=a2zt0000000TQNgAAO&status=Active	Rechenzentrumsdienstleistungen