Vertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

zwischen dem Auftraggeber gemäß Hauptvertrag

und

Echometer GmbH, Tondernstraße 1, 48149 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 von Mitarbeitenden 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, die Wartung und die Weiterentwicklung von Software und den darin vom Auftraggeber oder seinen Mitarbeitern eingebrachten personenbezogenen Daten sowie Support für die Nutzer der Software und 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 Beschäftigten
- Innerhalb des Tools hinterlassene Notizen der Beschäftigten
- Einordnung von Beschäftigten in Team- und Organisationshierarchien
- Nutzungsdaten (z.B. Seitenaufrufe und Klicks)
- Verbindungs-Metadaten (z.B. IP-Adressen)

(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 mindestens vier Wochen im Voraus in Kenntnis. Der Auftraggeber erhält hierdurch die Möglichkeit, gegen den neuen Subunternehmer in Textform Einspruch zu erheben. 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-Standardvertragsklauseln).

(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.

(3) Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Einschränkung oder Löschung personenbezogener Daten oder einem Auskunftsersuchen an den Auftragnehmer (Anträge gemäß Art. 15 bis 21 DSGVO) wird der Auftragnehmer die betroffene Person unverzüglich an den Auftraggeber verweisen.

§ 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 Aufbewahrung 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.

(3) Der Auftragnehmer ist verpflichtet, dem Auftraggeber jeden Verstoß gegen datenschutzrechtliche Vorschriften oder gegen diesen Vertrag, die im Zuge der Verarbeitung durch ihn oder andere mit der Verarbeitung für den Auftraggeber betraute Personen erfolgt ist, unverzüglich mitzuteilen. Soweit der Auftragnehmer ferner dazu berechtigt ist, wird er den Auftraggeber unverzüglich darüber informieren, wenn eine Aufsichtsbehörde nach Art. 58 DSGVO gegenüber dem Auftragnehmer tätig wird und dies die Verarbeitung, die der Auftragnehmer im Auftrag des Auftraggebers erbringt, betrifft.

§ 12 Aktualisierung dieser Auftragsverarbeitungsvereinbarung

(1) Die Auftragsverarbeitungsvereinbarung inklusive der TOM kann fortlaufend aktualisiert werden, um neuen Gegebenheiten gerecht zu werden.

(2) Aktualisierungen der AVV und TOM werden spätestens vier Wochen vor Inkrafttreten mit dem Auftraggeber geteilt.

(3) Der Auftraggeber hat in dieser Zeit, der Aktualisierung in Schriftform zu widersprechen (bspw. via E-Mail an support@echometer.de). Erfolgt kein derartiger Widerspruch, gilt die Aktualisierung als akzeptiert und tritt in Kraft.

(4) Aktualisierungen dieser AVV als auch der angehängten TOM werden ausschließlich mit den jeweiligen in der Echometer-App hinterlegten Workspace-Admins via Email geteilt.

Anlage 1: Technische und organisatorische Maßnahmen der Echometer GmbH

§ 1 Allgemeine Angaben

Verantwortlicher	Robin Roschlau, Geschäftsführer (CIO) der Echometer GmbH
Datum	01.05.2023
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) 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	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 und wird regelmäßig aktualisiert	x	
Anti-Virus-Software vorhanden und wird regelmäßig aktualisiert	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	x	

Wiederverwendung		
Verschlüsselung von mobilen Datenträgern	x	

(3) 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	

(4) Weitergabekontrolle

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

(5) Eingabekontrolle

TOM	Vorhanden?	Bemerkung
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 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, unbefugtes Einloggen und Überschreiten von Befugnissen, Benutzung von Admin-Accounts, Warnungen über unbefugtes Eindringen etc.)	x	Soweit durch verwendete Software unterstützt

(6) Auftragskontrolle

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	

(7) 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	

(8) Trennungskontrolle

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

§ 3 Abschluss

Bemerkungen	Die Technischen und Organisatorischen Maßnahmen der Telekom Deutschland GmbH 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 01.05.2024 statt.

Anlage 2: Subunternehmer

Die Telekom Deutschland GmbH stellt die Hosting-Infrastruktur bereit, in der unsere Software läuft.

Telekom Deutschland GmbH
Landgrabenweg 151
53227 Bonn
Telefon: 0228 - 181 0

Datenschutzbeauftragter:
Herrn Dr. Claus D. Ulmer,
Friedrich-Ebert-Allee 140,
53113 Bonn,
datenschutz@telekom.de

Die TOMs der Telekom Deutschland GmbH sind online einsehbar unter https://geschaeftskunden.telekom.de/hilfe-und-service/hilfe-themen/dsgvo/otc-deutsch (Deutsch) oder https://geschaeftskunden.telekom.de/hilfe-und-service/hilfe-themen/dsgvo/otc-englisch (Englisch)

Für weitere Informationen zu Zertifizierungen der Telekom Deutschland GmbH siehe: https://open-telekom-cloud.com/en/security/data-protection-and-compliance

PostHog ist eine Plattform zur Produktentwicklung und -analyse, die es ermöglicht, im Rahmen des Release-Managements neue Features sequentiell ausrollen, ihre Stabilität zu gewährleisten und ihre Nutzung zu analysieren. Außerdem werden Daten für Support- und Analysezwecke verarbeitet.

PostHog Inc
2261 Market Street #4008, San Francisco, CA 94114

Datenschutzbeauftragter:
Charles Cook (VP Operations)
privacy@posthog.com

Es wird ausschließlich das EU-Hosting von PostHog genutzt. Die TOMs der PostHog Inc sind online einsehbar unter https://docs.google.com/document/d/1xfpP1SCFoI1qSKM6rEt9VqRLRUEXiKj9_0Tvv2mP928/edit (Englisch)

Für weitere Informationen zu Zertifizierungen der PostHog Inc siehe: https://posthog.com/handbook/company/security