AUFTRAGSVERARBEITUNGSVERTRAG FÜR DIE NUTZUNG DER SUSTAINABILL CLOUD PLATTFORM

zwischen

VERSO GmbH Agnes-Pockels-Bogen 180992 München Deutschland (”**Verso**”)

und

dem Unternehmen, das sich für die Nutzung der sustainabill Cloud Plattform erfolgreich registriert hat (”**Unternehmen**”)

- zusammen „**Parteien**“ und jeweils einzeln „**Partei**“ –

Dieser Auftragsverarbeitungsvertrag einschließlich seiner Anlagen („Auftragsverarbeitungsvertrag“) regelt die Verarbeitung personenbezogener Daten durch Verso als Auftragsverarbeiter des Unternehmens im Zusammenhang mit der Nutzung der sustainabill Cloud Plattform („sustainabill Cloud Plattform“) durch das Unternehmen.

Grundsätzlich werden viele der Datenverarbeitungsvorgänge im Rahmen der sustainabill Cloud Plattform seitens des Unternehmens und/oder seitens Verso in eigener Verantwortung durchgeführt. Für gewisse Datenverarbeitung im Rahmen der sustainabill Cloud Plattform, beispielsweise die Möglichkeit für das Unternehmen, Lieferanten auf die sustainabill Cloud Plattform zur Transparenzschaffung in der Lieferkette einzuladen und mittels individueller, vom Unternehmen bereitgestellter Fragebögen Informationen direkt von den Lieferanten des Unternehmens zu erheben und zu verarbeiten, handelt Verso als Auftragsverarbeiter für das Unternehmen.

Dieser Auftragsverarbeitungsvertrag wurde zuletzt im Mai 2023 aktualisiert.

1. ANWENDUNGSBEREICH

1.1. Sofern und soweit Verso im Rahmen der Leistungserbringung personenbezogene Daten des Unternehmens im Auftrag verarbeitet, schließen die Parteien nachfolgenden Vertrag zur Verarbeitung von Daten im Auftrag entsprechend der Standardvertragsklauseln der EU Kommission vom 4. Juni 2021 nach Art. 28 (7) DSGVO (Durchführungsbeschluss (EU) 2021/915; https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32021D0915&from=DE) („Standardvertragsklauseln“).

1.2. Im Übrigen verarbeitet Verso die personenbezogenen Daten im Rahmen der sustainabill Cloud Plattform als Verantwortlicher gem. Art. 4 Nr. 7 DSGVO. Sollten die Parteien einen Vertrag zur gemeinsamen Verantwortlichkeit nach Art. 26 DSGVO abschließen müssen, wird dieser zusätzlich separat zu diesem Auftragsverarbeitungsvertrag abgeschlossen.

1.3. Die Definitionen in den Nutzungsbedingungen der sustainabill Cloud Plattform gelten in diesem Auftragsverarbeitungsvertrag entsprechend, soweit die Begriffe nicht in diesem Auftragsverarbeitungsvertrag oder in den Standardvertragsklauseln definiert sind.

2. STANDARDVERTRAGSKLAUSELN DER EU KOMMISSION

Die Parteien vereinbaren, dass die Verarbeitung durch Verso im Anwendungsbereich dieses Auftragsverarbeitungsvertrags auf der Grundlage der Standardvertragsklauseln erfolgt. Die Standardvertragsklauseln werden daher mit folgenden Spezifizierungen in diesen Auftragsverarbeitungsvertrag einbezogen:

Klausel der Standardvertragsklauseln	Spezifizierung
1 lit. a	Klausel 1 lit. a soll wie folgt lauten: a) Mit diesen Standardvertragsklauseln (im Folgenden „Klauseln“) soll die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) sichergestellt werden.
5	Die Parteien vereinbaren, dass Klausel 5 nicht einbezogen wird.
7.7 lit. a	Die Parteien vereinbaren eine allgemeine schriftliche Genehmigung sowie eine Unterrichtungsfrist von vier Wochen.
8 lit. c (4)	Klausel 8 lit. c (4) soll wie folgt lauten: 4) Verpflichtungen gemäß Artikel 32 der Verordnung (EU) 2016/679.
9.1 lit. b	Klausel 9.1 lit. b soll wie folgt lauten:b) bei der Einholung der folgenden Informationen, die gemäß Artikel 33 Absatz 3 der Verordnung (EU) 2016/679 in der Meldung des Verantwortlichen anzugeben sind, wobei diese Informationen mindestens Folgendes umfassen müssen: [...]
9.1 lit. c	Klausel 9.1 lit. c soll wie folgt lauten:c) bei der Einhaltung der Pflicht gemäß Artikel 34 der Verordnung (EU) 2016/679, die betroffene Person unverzüglich von der Verletzung des Schutzes personenbezogener Daten zu benachrichtigen, wenn diese Verletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.
9.2	Der letzte Absatz von Klausel 9.2 soll wie folgt lauten:Die Parteien legen in Anhang III alle sonstigen Angaben fest, die der Auftragsverarbeiter zur Verfügung zu stellen hat, um den Verantwortlichen bei der Erfüllung von dessen Pflichten gemäß Artikel 33 und 34 der Verordnung (EU) 2016/679 zu unterstützen

Anhang I	Hinsichtlich Informationen zum Verantwortlichen:Unternehmen, das sich für die Nutzung der sustainabill Cloud Plattform erfolgreich registriert hat und das die Nutzungsbedingungen mit Verso abgeschlossen hat (wie im Rahmen der Registrierung für die sustainabill Cloud Plattform identifiziert)Hinsichtlich Informationen zum Auftragsverarbeiter:Name und Anschrift: VERSO GmbH Agnes-Pockels-Bogen 180992 München Deutschland-Name, Funktion und Kontaktdaten der Kontaktperson: Klaus Wiesen, Geschäftsführer, Im Mediapark 5, 50670 Köln, klaus.wiesen@sustainabill.de .
Anhänge II und III	Siehe Anhänge A und B zu diesem Dokument.
Anhang IV	Die Parteien vereinbaren eine allgemeine schriftliche Genehmigung, sodass Anhang IV der Standardvertragsklauseln nicht auszufüllen ist.

Mit dem Abschluss genehmigt der Verantwortliche folgende Unterauftragsverarbeiter:

Name	Beschreibung der Verarbeitung
Telekom Deutschland GmbH, Landgrabenweg 151, 53227 Bonn	Betrieb der technischen Infrastruktur, sowie die Erstellung und Aufbewahrung von Backups.
Mapbox, Incorporated, 5th Floor 740 15th Street Northwest, Washington, DC 20005 („Mapbox“)	Darstellung von Karten und Geocoding (Ermittlung von Längen- und Breitengrad zu Adressen). (Hinweis: Je nach Internetverbindung und Einstellung kann die IP-Adresse des Nutzers übermittelt werden. Ausschließlich beim Geocoding werden weitere potenziell persönliche Daten (Adressen) an Mapbox gesendet.)
Mailjet SAS, 13-13 bis, Rue de l'Aubrac, 75012 Paris, France	Senden von E-Mails und die damit einhergehende Verarbeitung von E-Mail-Adressen und ggf. Namen.
Freshworks GmbH, Freshworks Inc., 2950 S. Delaware Street, Suite 201, San Mateo, CA 94403, USA	Kundenanfragen beantworten und sicherstellen, dass unsere Supportmitarbeiter stets über den Status aller offenen Supportanfragen informiert sind und die damit einhergehende Verarbeitung von E-Mail-Adressen und ggf. Namen.

Microsoft Corporation, One Microsoft Way, Redmond, WA 98052, USA	Empfangen von und Senden von persönlichen E-Mails (z.B. bei Premium Support) und ggf. Speichern von Projektdaten (z.B. Excel Listen von Kunden) sowie die damit einhergehende Verarbeitung von E-Mail-Adressen und ggf. Namen.

ANHANG A - Beschreibung der Verarbeitung

Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden:

- Lieferanten des Unternehmens (soweit diese natürliche Personen sind oder sich die Daten auf natürliche Personen beziehen)
- Mitarbeiter von Lieferanten des Unternehmens

Kategorien personenbezogener Daten, die verarbeitet werden:

- Kontaktdaten zum Lieferanten, die vom Unternehmen auf der sustainabill Cloud Plattform zur Verfügung gestellt werden, insbesondere Name des Lieferanten, E-Mail-Adresse, Website, und DUNS-Nummer
- Kontaktdaten zum Mitarbeiter des Lieferanten, die vom Unternehmen auf der sustainabill Cloud Plattform zur Verfügung gestellt werden, insbesondere Vor- und Nachname, E-Mail-Adresse und Job-Titel des Lieferanten
- Ggf. Nachhaltigkeits- und Transparenzangaben zum Lieferanten in individuellen Fragebögen, die vom Unternehmen stammen und deren Beantwortung der Unternehmer von seinen Lieferanten erbittet (soweit das Unternehmen diese Funktion der sustainabill Cloud Plattform nutzt)

Verarbeitete sensible Daten (falls zutreffend) und angewandte Beschränkungen oder Garantien, die der Art der Daten und den verbundenen Risiken in vollem Umfang Rechnung tragen, z. B. strenge Zweckbindung, Zugangsbeschränkungen (einschließlich des Zugangs nur für Mitarbeiter, die eine spezielle Schulung absolviert haben), Aufzeichnungen über den Zugang zu den Daten, Beschränkungen für Weiterübermittlungen oder zusätzliche Sicherheitsmaßnahmen:

Keine

Art der Verarbeitung:

Verso stellt dem Unternehmen die sustainabill Cloud Plattform zur Verfügung, um das Unternehmen dabei zu unterstützen, Nachhaltigkeits- und Compliance-Aspekte bei Lieferanten zu prüfen und die Transparenz der Lieferkette zu erhöhen. Die oben aufgelisteten personenbezogenen Daten werden von Verso im Auftrag des Unternehmens in der sustainabill Cloud Plattform gespeichert und nach Weisung des Unternehmens verarbeitet.

Zweck(e), für den/die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden:

- Einladung von Lieferanten auf die sustainabill Cloud Plattform durch das Unternehmen
- Einladen von Kollegen auf die sustainabill Cloud Plattform durch Mitarbeiter des Unternehmens
- Speicherung von Nachhaltigkeits- und Transparenzangaben zum Lieferanten in individuellen Fragebögen auf der sustainabill Cloud Plattform (soweit das Unternehmen

diese Funktion der sustainabill Cloud Plattform nutzt)

Dauer der Verarbeitung:

Eine Verarbeitung erfolgt in der Regel, bis die Nutzungsbedingungen der sustainabill Cloud Plattform gekündigt und das Vertragsverhältnis beendet wurde.

Bei der Verarbeitung durch (Unter-)Auftragsverarbeiter sind auch Gegenstand, Art und Dauer der Verarbeitung anzugeben.

Siehe oben unter Ziffer 2 des Haupttextes sowie diesem Anhang A.

ANHANG B - Technische und organisatorische Maßnahmen, einschließlich zur Gewährleistung der Sicherheit der Daten

Beschreibung der von dem/den Verantwortlichen ergriffenen technischen und organisatorischen Sicherheitsmaßnahmen (einschließlich aller relevanten Zertifizierungen) zur Gewährleistung eines angemessenen Schutzniveaus unter Berücksichtigung der Art, des Umfangs, der Umstände und des Zwecks der Verarbeitung sowie der Risiken für die Rechte und Freiheiten natürlicher Personen. Beispiele für mögliche Maßnahmen:

Der sustainabill Cloud-Service wird ausschließlich auf der Infrastruktur der Open Telekom Cloud (OTC) mit Sitz in Deutschland gehostet. Zusätzlich nutzen wir einen Backup- und Hochverfügbarkeitsstandort der OTC in den Niederlanden, um die Datenverfügbarkeit und Datenintegrität sicherzustellen.

Intern nutzt Verso die Office 365-Infrastruktur (O365) von Microsoft für E-Mail, (gemeinsame) Datenspeicherung und Kommunikation. Diese wird in der Europäischen Union gehostet.

Es werden keine personenbezogenen Daten der Kundinnen und Kunden von Verso in den eigenen Räumlichkeiten gespeichert oder verarbeitet, mit Ausnahme der Laptops der Mitarbeitenden.

Die folgenden TOMs beschränken sich daher auf Maßnahmen, um die Cloud-Serviceprovider abzusichern und auf die in den eigenen Räumlichkeiten getroffenen Sicherheitsmaßnahmen. Die physische Absicherung und Maßnahmen, die von unseren Hostern durchgeführt werden, finden Sie in der folgenden Dokumentation:

- https://open-telekom-cloud.com/en/security/data-protection-and-compliance (OTC) und
- https://docs.microsoft.com/en-us/compliance/regulatory/gdpr (O365)

Alle kundenorientierten Unterauftragsverarbeiter werden in unserer Datenschutzerklärung aufgeführt.

VERTRAULICHKEIT

Zutrittskontrolle

Maßnahmen, die verhindern, dass Unbefugte Zugang zu Datenverarbeitungssystemen erhalten, mit denen personenbezogene Daten verarbeitet werden:

- In unseren Räumlichkeiten werden keine Kundendaten gespeichert/aufbewahrt
- Schlüsselvergabe an Mitarbeiter mit Übergabeprotokoll
- Türsicherung (elektrischer Türöffner zum Öffnen der Räumlichkeiten, physischer Schlüssel zu Büro(s))

- Sorgfältige Auswahl von Dienstleistern und Subunternehmern durch Startplatz Köln
- Clean Desk Policy (keine Verträge oder sensible Daten auf dem Schreibtisch erlaubt, wenn der Schreibtisch verlassen wird)
- Dokumentenvernichter und Richtlinie zum Vernichten von Dokumenten mit personenbezogenen Daten, wenn eine Archivierung nicht gesetzlich erforderlich ist
- Sichere Löschung von (externen) Laufwerken

Zugangskontrolle und Zugriffskontrolle

Maßnahmen, die verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden.

Die meisten Maßnahmen beziehen sich auf die Laptops und Telefone der Mitarbeiter und/oder die Schnittstellen zur Serverinfrastruktur. Server und die Speicherinfrastruktur sind vollständig gehostet (s. oben):

- Alle Systeme sind passwortgeschützt
- Passwortrichtline für sichere Passwörter
- Alle Festplatten von Desktop- und Laptop-Computern sind vollständig verschlüsselt
  - Tragbare Geräte werden in unser MDM System zur Fernsperrung und -löschung integriert
- Entwicklungs- und Verwaltungssysteme sind besonders gesichert, z.B.
  - Nutzung von MFA insofern möglich, insbesondere für O365 (z. B. E-Mail und Dateien)
  - Klare Richtlinien zur Auswahl von Cloud-Anbietern
- Jeder Mitarbeiter nutzt Firmenhardware (keine "Bring your own device"-Policy)
- Organisatorische Maßnahmen bei Beendigung des Arbeitsverhältnisses (u.a.: Zugang wird bei allen Cloud-Anbietern systematisch gelöscht, Hardware des Mitarbeiters wird zurückgegeben und vollständig gelöscht)
- Daten werden ausschließlich über eine TLS/SSL-verschlüsselte Verbindung übertragen
- Protokollierung von Datenveränderungen in der sustainabill Cloud
- Protokollierung von Datenveränderungen in Microsoft O365
- Die Vergabe von Berechtigungen erfolgt immer nach dem „Need to Know"-Prinzip
- Zugriffsrechte auf persönliche/sensible Daten können nur von Administratoren verwaltet werden
- Die Anzahl der Administratoren ist bei jedem Dienst (auch SaaS) immer auf ein Minimum beschränkt

Darüber hinaus setzt Verso auf eine bedarfsgerechte Gestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung.

PSEUDONÜMISIERUNG

Technische Maßnahmen	Organisatorische Maßnahmen

Ersetzen von IP-Adressen in Protokollen, die älter als ein Monat sind	Wenn möglich und nicht anders gesetzlich verlangt, werden personenbezogene Daten nicht gespeichert (z.B. durch Entfernen von Namen, E-Mails-Adressen, ...)

INTEGRITÄT

Übertragungskontrolle

Der Austausch personenbezogener Daten erfolgt ausschließlich innerhalb unserer Infrastruktur bzw. der unserer Unterauftragsverarbeiter. Zwischen den einzelnen Systemen werden die Daten entweder lokal oder über eine SSL-verschlüsselte Datenverbindung übertragen.

Personenbezogene Daten werden im Zuge der Übertragung und Verarbeitung nicht verändert und bleiben unversehrt, vollständig und aktuell. Wir übernehmen alles Notwendige, um zu verhindern, dass Daten verfälscht oder falsche Daten verarbeitet werden. Gleichzeitig wird sichergestellt, dass Änderungen an Daten nachvollzogen werden können, z.B. durch Versionierung oder Log-Dateien.

Technische Maßnahmen	Organisatorische Maßnahmen
Sicherstellen, dass die Verbindungen zu allen Cloud-Anbietern nach dem neuesten Stand der Technik verschlüsselt sind.	Sicherstellen, dass bei der Archivierung von Daten personenbezogene Daten pseudonymisiert oder entfernt werden (insofern gesetzlich nicht anders verlangt).
Sicherstellen, dass alle Daten auf den offiziellen IT-Systemen übertragen werden (Prävention von Schatten-IT).	Sicherstellen, dass archivierte Daten nur von Administratoren und/oder berechtigten Personen eingesehen werden können

EINGABEKONTROLLE

Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, geändert oder entfernt (gelöscht) wurden.

Personenbezogene Daten können jederzeit ihrer Herkunft zugeordnet werden und können nur vom Auftraggeber (und dessen Nutzern) sowie vom Verso Support angelegt und/oder bearbeitet werden. Bei jeder Änderung wird der Benutzer sowie ein Zeitstempel protokolliert. Darüber hinaus erfolgt eine Protokollierung über Log Dateien.

Technische Maßnahmen	Organisatorische Maßnahmen
Technische Protokollierung der Dateneingabe, -änderung und -löschung durch Historisierung und Log Dateien	Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können
Manuelle und automatisierte Kontrolle von Log Dateien	Nachvollziehbarkeit der Eingabe, Änderung und Löschung von Daten über einzelne Benutzernamen (nicht Benutzergruppen)

	Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

Trennungskontrolle / Datenseparierung

Maßnahmen zur Sicherstellung der getrennten Verarbeitung (Speicherung, Änderung, Löschung, Übermittlung) von Daten mit unterschiedlichem Zweck.

Die sustainabill Cloud wird von mehreren Kundinnen und Kunden gleichzeitig genutzt (sie ist mandantenfähig) und gewährleistet eine logische Trennung der Daten.

Zusätzlich trennen wir unser Entwicklungssystem, Testsystem und Produktivsystem, um sicherzustellen, dass Daten aus dem Produktivsystem nur von berechtigten Personen eingesehen werden können.

Wir nutzen unterschiedliche Systeme zu unterschiedlichen Zwecken (z.B. zur Abrechnung, Akquise, internen Datenverarbeitung, etc.). Diese Systeme werden nicht miteinander verbunden und sind physisch separiert, insofern eine Verbindung der Systeme (z.B. über APIs) nicht zwingend für die Verarbeitung notwendig ist.

Verfügbarkeitskontrolle

Maßnahmen zum Schutz personenbezogener Daten vor versehentlicher Zerstörung oder Verlust finden Sie in der OTC- und O365-Dokumentation (s. oben).

Zusätzlich zu den Maßnahmen unserer Unterauftragnehmer, stellen wir Folgendes sicher:

Technische Maßnahmen	Organisatorische Maßnahmen
Einsatz von Hochverfügbarkeitsclustern (OTC managed K8S) für die sustainabill Cloud Backup- und Recovery-Konzepte	Regelmäßige, mindestens tägliche Backups Getrennte Laufwerke und wenn möglich getrennte Server für Betriebssysteme und Daten in der sustainabill Cloud

VERFAHREN ZUR ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG

Datenschutz-Management

Technische Maßnahmen	Organisatorische Maßnahmen
Zentrale Implementierung und Dokumentation aller Zugriffsberechtigungen für Mitarbeiter	Regelmäßige Sensibilisierung der Mitarbeiter, mindestens halbjährlich Regelmäßige Überprüfung der Berechtigungen nach dem „Need to Know“-Prinzip

Reaktion auf Vorfälle

Im Falle eines Datenschutzvorfalls wird der folgende interne Prozess eingeleitet:

- Untersuchung von Umfang und Ursache des Vorfalls
  - Wenn personenbezogene Daten betroffen sind, werden die betroffenen Kunden spätestens innerhalb von 48 Stunden nachdem der Vorfall von uns registriert wurde.

    - Im Falle eines Datenverlustes: Teilwiederherstellung, falls zutreffend, oder Rollback auf die letzte Vollsicherung (max. 24 Stunden Datenverlust möglich)
    - Tägliche Benachrichtigung der Kunden über den Status
- Nach Behebung der Ursache eines Vorfalls, verbessern wir die Absicherung der Systeme in Bezug auf die identifizierte(n) Sicherheitslücke(n)

Datenschutzfreundliche Einstellungen

Als Plattform, die für Transparenz steht, ist es unser Anliegen, das Kundinnen und Kunden sich aktiv für die Weitergabe ihrer Daten entscheiden können. D.h. Kunden können in jeder Situation explizit entscheiden, ob Daten geteilt werden oder sich entscheiden, dass bestimmte Daten immer geteilt werden.

Wir überprüfen unsere Prozesse und Schnittstellen im Hinblick auf die Darstellung und Verarbeitung von personenbezogenen Daten regelmäßig und versuchen eine solche Darstellung und Verarbeitung zu minimieren.