## PROCESSING AGREEMENT FOR USE OF THE SUSTAINABILL CLOUD PLATFORM

Between

VERSO GmbH Agnes-Pockels-Bogen 180992 München Germany ("**Verso**")

and

The company that successfully registered to use the sustainabill Cloud Platform ("**Company**")

- referred to together hereinafter as the "**Parties**" and, individually, as a "**Party**" –

This Processing Agreement, including its Annexes, ("Processing Agreement") governs the processing of personal data by Verso as the processor of the Company in relation to the Company's use of the sustainabill Cloud Platform ("sustainabill Cloud Platform"). Data on the sustainabill Cloud Platform is normally processed by the Company and/or Verso. For certain processing on the sustainabill Cloud Platform, e.g., the Company's option to invite suppliers to the sustainabill Cloud Platform for supply chain transparency and to collect and process information directly from suppliers by using Company surveys, Verso will serve as the processor on behalf of the Company.

*This processing agreement was last updated in May 2023.*

### 1. APPLICATION

1.1. Where Verso processes personal data on behalf of the Company as part of service performance, the Parties conclude this Agreement on the processing of data on behalf of the Company in accordance with the standard contractual clauses of the European Commission of 4 June 2021 pursuant to Article 28(7) of the EU GDPR (Commission Implementing Decision (EU) 2021/915; https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021D0915&from=EN) ("standard contractual clauses").

1.2. Apart from that, Verso processes personal data on the sustainabill Cloud Platform as the controller within the meaning of Article 4(7) of the EU GDPR. Should the Parties have to conclude a joint controller agreement within the meaning of Article 26 of the EU GDPR, this agreement will be concluded separately of this Processing Agreement.

1.3. Where terms are not defined in this Processing Agreement or in standard contractual clauses, the definitions in the Terms of Use of the sustainabill Cloud Platform apply.

### 2. STANDARD CONTRACTUAL CLAUSES OF THE EUROPEAN COMMISSION

The Parties agree that any processing by Verso will be governed by this Processing Agreement on the basis of the standard contractual clauses. The standard contractual clauses are therefore included in this Processing Agreement with the following specifications:

| Standard Contractual Clause | Specification |
|---|---|

| | |
|---|---|
| 1(a) | Clause 1(a) should be as follows:a) These standard contractual clauses (hereinafter "Clauses") shall ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). |
| 5 | The Parties agree that Clause 5 shall be waived. |
| 7.7(a) | The Parties agree to require general written permission and a notice period of 4 weeks. |
| 8(c)(4) | Clause 8(c)(4) should be as follows:4) Obligations under Article 32 of Regulation (EU) 2016/679. |
| 9.1(b) | Clause 9.1(b) should be as follows:b) when obtaining the following information which must be included in notification of the controller under Article 33(3) of Regulation (EU) 2016/679 and which must at least include the following ... |
| 9.1(c) | Clause 9.1(c) should be as follows:c) for compliance with the obligation under Article 34 of Regulation (EU) 2016/679 to communicate any breach of personal data to the data subject without undue delay where the breach is likely to result in a high risk to the rights and freedoms of natural persons. |
| 9.2 | The last paragraph of Clause 9.2 should be as follows:Any other information to be provided by the processor to assist the controller with the performance of the obligations under Article 33 and Article 34 of Regulation (EU) 2016/679 is specified by the Parties in Annex III. |

| | |
|---|---|
| Annex I | Concerning information about the controller:The Company which successfully registered to use the sustainabill Cloud Platform and agreed to the Terms of Use with Verso (as identified as part of the registration for the sustainabill Cloud Platform)Concerning information about the processor:Name and address: VERSO GmbH Agnes-Pockels-Bogen 180992 München GermanyName, function, and contact details of contact person: Klaus Wiesen, CEO, Im Mediapark 5, 50670 Cologne, Germany, klaus.wiesen@sustainbill.de . |
| Annexes II and III | See Annexes A and B to this document. |
| Annexes IV | The Parties agree on general written permission so that Annex IV to the Standard Contractual Clauses does not have to be completed. |

**Concluding this document, the controller approves the following sub-processors:**

| Name | Beschreibung der Verarbeitung |
|---|---|
| Telekom Deutschland GmbH, Landgrabenweg 151, 53227 Bonn | Operating the technical infrastructure and creating and storing backups |
| Mapbox, Incorporated, 5th Floor 740 15th Street Northwest, Washington, DC 20005 („Mapbox“) | Display of maps and geocoding (i.e. the determination of longitude and latitude to addresses). (Note: Depending on the Internet connection and settings, the user's IP address may be transmitted. Only geocoding sends other potentially personal information (addresses) to Mapbox). |
| Freshworks GmbH, Freshworks Inc., 2950 S. Delaware Street, Suite 201, San Mateo, CA 94403, USA | Respond to customer inquiries and ensure that our support staff is always aware of the status of all open support requests. This includes the processing of email addresses and names, if applicable. |
| Mailjet SAS, 13-13 bis, Rue de l'Aubrac, 75012 Paris, France | Sending emails and processing email addresses and, if applicable, names. |
| Microsoft Corporation, One Microsoft Way, Redmond, WA 98052, USA | Receiving and sending personal emails (e.g. for Premium Support) and, if applicable, storing project data (e.g. Excel lists) as well as the associated processing of email addresses and, if applicable, names. |

**ANNEX A - Description of Processing**

*Categories of data subjects whose personal data is processed:*

- The Company's suppliers (if these are or the data refers to natural persons)
- Employees of the Company's suppliers

*Categories of personal data that is processed:*

- Suppliers' contact details provided by the Company on the sustainabill Cloud Platform, especially the name of the supplier, email address, website, and DUNS number
- Contact details of employees of the Company's suppliers provided by the Company on the sustainabill Cloud Platform, especially the first and last name, email address and Job title of the supplier
- If applicable, information about suppliers' sustainability and transparency provided on surveys of the Company and which the Company asks suppliers to complete (if the Supplier uses this function of the sustainabill Cloud Platform)

*Processed sensitive data (if applicable) and applied restrictions or guarantees that fully consider the type of data and related risk, e.g., strict purpose limitation, access restriction (including limiting access to employees who completed special training), data access logs, restrictions on transmissions or other security measures:*

None

*Type of processing:*

Verso offers the sustainabill Cloud Platform to help the Company review sustainability and compliance aspects of suppliers and increase the transparency of the supply chain. The personal data listed above is stored by Verso on the sustainabill Cloud Platform on behalf of and processed as instructed by the Company.

*Purpose(s) for which personal data is processed on behalf of the controller:*

- Invitation of the Company to suppliers to join the sustainabill Cloud Platform
- Invitation of the Company's employees to colleagues to join the sustainabill Cloud Platform
- Saving information about sustainability and transparency from supplier surveys on the sustainabill Cloud Platform (if the Company uses this function of the sustainabill Cloud Platform)

*Duration of Processing:*

Data is normally processed until the Terms of Use of the sustainabill Cloud Platform are terminated and the contractual relationship ends.

*For data processed by (sub-)processors, the subject, type and duration of processing must be stated.*

See above Section 2 of the main text, and this Annex A.

**ANNEX B - Technical and Organizational Measures, Including for Safeguarding the Security of Data**

*Description of the technical and organizational security measures (including any relevant certification) implemented by the controller to ensure an adequate level of protection in consideration of the nature, scope, context and purposes of processing and the risk to the rights and freedoms of natural persons. Examples of possible measures:*

The sustainabill Cloud Service is hosted exclusively on the infrastructure of the Open Telekom Cloud (OTC) based in Germany. We also use an OTC backup and high-availability site in the Netherlands to ensure data availability and integrity.

Internally, Verso uses the Office 365 infrastructure (O365) of Microsoft for emails, (joint) data storage and communication. This infrastructure is hosted in the European Union.

Personal data of Verso's clients is not stored or processed at Verso's offices, except on laptops of employees.

The following TOMs are therefore limited to measures for securing the Cloud service provider and to the security measures at Verso's offices. For the physical security and measures performed by our hosts, please see the following documentation:

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

All client-based sub-processors are listed in our Privacy Policy.

**CONFIDENTIALITY**

**Entrance Control**

*Measures to prevent unauthorized access to data processing systems processing personal data:*

- No client data saved/stored at our offices
- Keys issued to employees with handover documentation
- Door protection (electric door opener, physical key to office(s))
- Careful selection of service providers and subcontractors by STARTPLATZ Cologne
- Clean desk policy (no contracts or sensitive data permitted on desk after leaving)
- Shredder, policy for shredding documents with personal data where archiving is not required by law
- Secure erasure of (external) drives

**Retrieval Control and Access Control**

*Measures to prevent unauthorized use of data processing systems.*

Most measures refer to the laptops and telephones of employees and/or to server infrastructure interfaces. Servers and the storage infrastructure are fully hosted (see above):

- All systems password-protected
- Password policy for secure passwords
- All desktop and laptop hard disks fully encrypted
    - Portable devices only integrated into our MDM system for remote locking and erasure
- Development and administrative systems specially protected though, e.g.,
    - Use of MFA where possible, especially for O365 (e.g., email and files)
    - Clear policy for choosing Cloud providers
- All employees using company hardware (no "bring your own device" policy)
- Organizational measures when terminating employment (e.g., systematically deleting all Cloud provider access, returning and completely deleting employee's hardware)

- Transmitting data only via TLS/SSL-encrypted connections
- Logging file changes on sustainabill Cloud
- Logging file changes on Microsoft O365
- Granting authorization only according to "need to know" principle
- Access rights to personal/sensitive data administered only by administrators
- Number of administrators limited to minimum for each service (incl. SaaS)

Furthermore, Verso uses a need-based authorization concept and access rights which are also monitored and logged.

**PSEUDONYMIZATION**

| Technical Measures | Organizational Measures |
|---|---|
| Replacing IP addresses in protocols older than 1 month | If possible and not required otherwise by law, not storing personal data (e.g., by removing names, email addresses, ...) |

**INTEGRITY**

**Transmission Control**

Personal data is only exchanged within our or our sub-processors' infrastructure. Data is transmitted between systems either locally or via an SSL-encrypted connection.

Personal data is not changed during transmission or processing and remains intact, complete, and up to date. We do anything necessary to prevent data from being processed incorrectly and incorrect data from being processed. We also ensure that any changes to data can be tracked, e.g., through versioning or log files.

| Technical Measures | Organizational Measures |
|---|---|
| Ensuring that connections to all Cloud providers have state-of-the-art encryptions. | Ensuring pseudonymization or removal of personal data when archived (unless required otherwise by law). |
| Ensuring that all data is transmitted on official IT systems (shadow IT prevention). | Ensuring that archived data can only be read by administrators and/or authorized persons. |

**INPUT CONTROL**

*Measures to subsequently determine whether and by whom data was entered, changed or removed (deleted).*

Personal data can be assigned to its source at any time and may only be entered and/or edited by the client (and the client's users) and Verso support service. When making any changes, the user and the timestamp are logged in log files.

| Technical Measures | Organizational Measures |
|---|---|
| Technical logging of data input, changes and erasure through historization and log files | Overview of which data may be entered, changed or erased with which programs |

| | |
|---|---|
| Manual and automated log file control | Tracking input and erasure of and changes to data by username (not user groups)<br>Granting rights to enter, change and erase data based on an authorization concept |

**Separation Control / Data Separation**

*Measures to ensure separate processing (storage, changes, erasure, transmission) of data processed for different purposes.*

The sustainabill Cloud is used by several clients simultaneously (client capacity) and ensures a logical separation of data.

We also separate our development system, test system and productive system to ensure that data from the productive system may only be read by authorized persons.

We use different systems for different purposes (e.g., for accounting, acquisition, internal data processing, etc.). These systems are not connected to each other and are physically separate where connections between systems (e.g., APIs) are not necessary for processing.

**Availability Control**

*Measures that protect data against accidental loss or destruction are specified in the OTC and O365 documentation (see above).*

In addition to the measures of our subcontractors, we ensure the following:

| Technical Measures | Organizational Measures |
|---|---|
| Use of high-availability clusters (OTC-managed K8S) for the sustainabill Cloud | Backup and recovery concepts |
| Regular, at least daily backups | Separate drives and, where possible, separate servers for operating systems and files on the sustainabill Cloud |

**REVIEW, ASSESSMENT AND EVALUATION PROCEDURE**

**Data Protection Management**

| Technical Measures | Organizational Measures |
|---|---|
| Central implementation and documentation of all access authorization of employees | Regular, at least half-yearly employee sensitization |
| | Regular reviews of authorization based on “need to know” principle |

**Incident Response Management**

In case of data breaches, the following internal process is implemented:

- Determining scope and cause of incident
  - If personal data is affected, notifying affected clients, at the latest, within 48 hours of incident

    - In case of data loss: partial restoration, if possible, or rollback to last full backup (no possible loss of data older than 24 hours)
    - Daily communication of status to clients
- After rectifying cause of incident, improving system security regarding identified vulnerability

**Privacy by Design and Default**

As a platform that stands for transparency, we want our clients to be able to decide whether to share their data. This means that our clients can always decide whether to share data or to always share certain data.

We regularly review and try to minimize the display and processing of personal data by our processes and interfaces.