Annex I – Data Processing Agreement

This Data Processing Agreement is an annex to the Billit Terms and Conditions and forms an integral part of the Agreement between the Client and Billit.

This Annex I sets out the additional terms, requirements, and conditions under which Billit (acting in the capacity of Processor) will process Personal Data on behalf of the Client (acting in the capacity of Controller) (when providing Services) in the execution of the Agreement. This Annex I contains the mandatory clauses required by Article 28(3) of the General Data Protection Regulation 2016/679 (hereinafter referred to as "**GDPR**") for agreements between Controllers and Processors.

1. Definitions and Interpretation

1.1. The following definitions apply in this Annex I:

"**Business Purposes**" means the Services described in the Agreement and any other purposes specifically identified in Schedule A.

"**Data Protection Legislation**" means any Belgian and European data protection laws, including decisions, directives, and regulations, for the protection of personal data, particularly the GDPR and the relevant implementing legislation under Belgian law.

"**Controller**", "**Data Protection Impact Assessment**", "**Data Subject**", "**Personal Data**", "**Personal Data Breach**", and "**process/processing**" shall have the same meaning as in the GDPR.

1.2. Capitalized terms used in this Annex I but not defined herein shall have the meaning set forth elsewhere in the Agreement.

1.3. This Annex I shall be subject to the terms and conditions as set out in the Billit Terms and Conditions and forms an integral part of the Agreement between the Parties.

1.4. In case of discrepancy between any of provisions of this Annex I and those of the Agreement, this Annex I shall prevail.

2. Types of Personal Data and Purposes of the Processing

2.1. In respect of the processing of Personal Data by Billit on the Client's behalf, the Client shall act as the Controller and Billit as the Processor as defined in the Data Protection Legislation.

2.2. The Controller shall retain control over the Personal Data and remain responsible for fulfilling its compliance obligations under the Data Protection Legislation, including making the required communications, adhering to its information obligations and obtaining the necessary consent, as well as for the processing instructions it gives to the Processor.

2.3. Schedule A describes the data processing details, including the nature of the Processor's processing, the categories of Personal Data, the categories of Data Subjects, and the storage periods for Personal Data.

3. Obligations of the Processor

3.1. The Processor shall process the Personal Data only in line with the Client's written instructions. The Processor shall not process the Personal Data for any other purpose or in a manner inconsistent with this Annex I or the Data Protection Legislation. The Processor shall inform the Client immediately if it considers that the Client's instructions are not in line with the Data Protection Legislation. In said event, the Processor shall have the possibility to (i) suspend the implementation of the instruction in question until the Controller confirms, modifies or withdraws its instruction, or (ii) to terminate the Agreement or cooperation, if, after consultation, the Controller persists in the breach or the unlawful instruction.

3.2. The Processor shall keep all Personal Data confidential and shall not disclose them to third parties unless the Client or this Annex I has authorized such disclosure or it is required by law. If any law, court, regulatory body, or supervisory authority requires the Processor to process or disclose Personal Data, the Processor shall first notify the Client of such a legal or regulatory obligation and provide the Client with the opportunity to object to or challenge this obligation, unless such notification is prohibited by law.

3.3. The Processor shall provide reasonable and to the best of its abilities assistance to the Client in fulfilling the Client's compliance obligations under the Data Protection Legislation, taking into account the nature of the Processor's processing and the information available to the Processor, including with respect to the Data Subject's rights, Data Protection Impact Assessments as well as reporting to and consulting with supervisory authorities under the Data Protection Legislation.

3.4. The Client shall reimburse the Processor in accordance with Article 13 of this Annex I for services rendered in accordance with this Article 3, unless this assistance is the result of a proven non-compliance by the Processor with this Annex I.

4. Sub-processors

4.1. The Client herewith gives a general written authorization to the Processor to engage other Sub-processors under the following conditions:

a) If the Processor intends to appoint another Sub-processor, it shall inform the Client accordingly and allow the Client to object to this appointment within fourteen (14) days. This is on the provision that the Client may only object to such an appointment in writing and on reasonable grounds supported by documentary evidence. If the Controller did not submit a written, well-reasoned objection to the engagement of any additional Sub-Processors, upon receipt of the notification and within the aforementioned time, the engagement of the additional Sub-Processors shall be deemed authorized; and

b) The Processor shall enter into a written agreement with each Sub-processor containing, as to their subject matter, the same conditions as those in this Processing Agreement, specifically concerning the requirements for taking appropriate technical and organizational security measures. The Processor shall provide copies of such agreements to the Client on the Client's written request, provided however, that the Processor shall be entitled to blackline any business sensitive information.

4.2. The Sub-Processors approved at the commencement of this Annex I are set out in Schedule A. Upon request of the Controller, an updated list of engaged Sub-Processors shall be made available.

4.3. Subject to Article 14, the Processor shall remain fully liable to the Client for any failure by a Sub-processor to fulfil its obligations concerning the processing of the Personal Data pursuant to the applicable Data Protection Legislation.

5. Cross-border transfer of personal data

5.1. The Processor (or any Sub-Processor) shall not transfer or otherwise process Personal Data outside the European Economic Area (EEA) without obtaining the Controller's prior written consent. Such consent of the Controller is not required when the transfer of Personal Data to countries outside the EEA is mandatory under EU or EU member state provisions.

5.2. The Processor (or a Sub-processor) shall only transfer or otherwise process Personal Data outside the European Economic Area ("**EEA**") if the Processor (or the Sub-processor) has provided appropriate safeguards pursuant to Article 46 GDPR.

5.3. If applicable, the Processor (or the Sub-processor) shall enter into EU standard contractual clauses with the data importer outside the EEA as approved by the European Commission or by implementing any other instruments approved by the European Commission that ensure that the transfer of Personal Data to a country outside the EEA complies with appropriate safeguards as required by the GDPR.

6. Confidentiality

6.1. The Processor shall ensure that all employees who are authorized to process the Personal Data:

a) are bound by appropriate obligations of confidentiality and usage restriction in respect of the Personal Data; and

b) are aware of the Processor's and their own personal obligations pursuant to the Data Protection Legislation.

7. Security

7.1. The Processor shall take appropriate technical and organizational measures in accordance with Article 32 GDPR, as further described in Schedule A. In assessing the appropriate level of security, due account shall be taken of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the Data Subjects.

7.2. The Controller shall provide sufficient guarantees regarding the implementation of appropriate technical and organizational measures so that the processing complies with the requirements set out in the GDPR and so that the protection of the rights of Data Subjects is ensured. In particular, the Controller shall only make personal data available to the Processor for processing if it has verified that the appropriate security measures are in place.

7.3. In implementing these security measures, the Processor shall take into account applicable standards, including but not limited to ISO/IEC 27001 (Information Security Management Systems) and ENISA guidance on data protection and cybersecurity. While formal certification is not required, the Processor shall maintain security controls that are at least materially equivalent to those prescribed in ISO/IEC 27001.

7.4. More information & the ISO/IEC 27001 certificate is available on our focus on Compliance & Trust is available at https://www.billit.eu/en-int/about-us/compliance-trust

8. Audits

8.1. The Processor shall provide the Client with all information, reasonably necessary, to demonstrate compliance with the obligations pursuant to this Annex I and the Data Protection Legislation and shall permit and cooperate with audits executed by the authorized auditors of the Client, regarding the Processor's compliance with this Annex I.

8.2. Such audits may only be carried out if the Processor has been notified by a registered letter at least thirty (30) days in advance. Audits may be conducted up to once per contract year (or in case there are objective and serious indications that the Processor breaches its obligations under this Annex I), on any day (between 9.00 am and 6.00 pm), except Saturdays, Sundays, statutory holidays in Belgium, and days when the Processor is closed due to holidays. Audits shall not unreasonably interfere with the Processor's business activities. The Controller's confidentiality obligations towards third parties must be taken into account when conducting such an audit. Both the Controller and its auditors shall keep the information disclosed in the context of an audit confidential and shall only use it for the purpose of verifying the Processor's compliance with this Annex I. Audits shall always be carried out at the Client's expense, unless the audit demonstrates non-compliance with this Annex I by the Processor. The Processor is entitled to request that the Client and external auditor sign a non-disclosure agreement before the audit is carried out.

8.3. The findings of the audit will be assessed by the Processor and the Client in mutual consultation and, will (if necessary) lead to the implementation of adjustments by the Processor and/or the Client, as far as this is reasonable in the context of the performance of the Agreement. The Processor and Client shall have the possibility to (i) suspend the implementation of the instruction in question until the instructions are confirmed, modified or withdrawn, or (ii) to terminate the Agreement or cooperation, if, after consultation, the relevant Party persists in a unreasonable instruction or in the breach or the unlawful instruction.

8.4. The costs incurred by the Processor for assisting in such audits shall be reimbursed by the Client in accordance with Article 13 of this Annex I unless expressly agreed otherwise in writing or the audit demonstrates non-compliance with this Annex I by the Processor.

9. Information and Assistance

9.1. The Processor shall take the appropriate technical and organizational measures agreed in writing between the Parties and shall promptly provide the Client with the information that the Client may reasonably require to enable the Client to comply with:

a) Data Subject requests pursuant to the Data Protection Legislation; and

b) Information or assessment notices served by a supervisory authority on the Controller under the Data Protection Legislation.

9.2. The Processor shall inform the Client without undue delay (i.e. five (5) Business Bays) if it receives a complaint, notification, or communication directly or indirectly relating to the processing of the Personal Data or one of the Parties' compliances with the Data Protection Legislation.

9.3. The Processor shall inform the Client within five (5) Business Days if it receives a request from a Data Subject to access their Personal Data or to exercise any of their rights under the Data Protection Legislation.

9.4. The Processor shall reasonably and to the best of his abilities cooperate and assist the Controller in responding to complaints, notifications, communications, or requests from Data Subjects. For the avoidance of doubt, the Processor shall not directly respond to the Data Subject request itself, unless expressly authorized in writing to do so by the Controller.

9.5. The costs incurred by the Processor for aiding under this Article shall be reimbursed by the Client in accordance with Article 13 of this Annex I.

10. Personal Data Breach

10.1. The Processor shall inform the Client without undue delay and in any event within seventy-two (72) hours if it becomes aware of a Personal Data Breach.

10.2. If the Processor becomes aware of a Personal Data Breach, it shall provide the Client with the following information without undue delay:

a) A description of its nature, including the categories and estimated number of Data Subjects and Personal Data records affected;

b) The likely consequences;

c) The details of a contact point where more information can be obtained;

d) A description of the measures taken or proposed to address the Personal Data Breach including those to mitigate its possible adverse effects; and

e) the (alleged) cause, the date on which the Personal Data Breach occurred (if no exact date is known: the period within which the Personal Data Breach occurred) and the date and time on which the breach became known to the processor or to a Sub-Processor engaged by it.

Where and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

10.3. Immediately following a Personal Data Breach, the Parties shall work together to investigate the Personal Data Breach. The Processor shall reasonably cooperate with the Client in dealing with the Personal Data Breach, including by:

a) Cooperating in an investigation; and

b) Taking reasonable and prompt steps to mitigate the consequences of and minimize any damage caused by the Personal Data Breach.

10.4. The Processor shall refrain from notifying third parties of a Personal Data Breach without the Client's prior written consent unless it is required to do so by law. It is and remains the responsibility of the Client to report (if applicable) a Personal Data Breach to the competent supervisory authority and/or the Data Subject.

10.5. The Client shall cover all reasonable costs related to the Processor's performance under this Article in accordance with Article 13 of this Annex I, unless the Personal Data Breach is due to the Processor's negligence, willful misconduct, or breach of this Annex I.

11. Term and Termination

11.1. This Annex I shall remain in full force and effect as long as:

a) The Agreement remains in force; or

b) The Processor holds or controls Personal Data in connection with the Agreement (hereinafter referred to as the "**Term**").

11.2. Any provision of this Annex I which is to become or remain effective, either expressly or tacitly, upon or after the termination of the Agreement (including Article 14) shall remain in full force and effect.

12. Removal or Return

12.1. Upon termination of the Agreement, for whatever reason, the Processor shall, at the Client's discretion, delete or return all the Personal Data that are in its possession, and delete any existing copies, unless the Processor must retain such Personal Data for a longer term pursuant to applicable law.

13. Costs

13.1. The services performed under this Annex I for which the Processor may charge the Client will be charged on the basis of the amount of hours worked and the Processor's then standard hourly rates. Upon request, the Processor shall inform the Controller of its standard rates. The Processor will invoice these amounts on a monthly basis in accordance with the payment modalities set forth in the Agreement. For the avoidance of doubt, only the services executed by the Processor to ensure the Controller can adhere to its obligations under the Data Protection Legislation shall be charged. Services provided by the Processor under this Annex I to ensure the Processor adheres to its own obligations under the Data Protection Legislation, shall not be reimbursed, unless expressly agreed otherwise in writing. All payments by the Controller to the Processor shall be executed in accordance with the terms of the Agreement.

14. Final Provisions

14.1. To the extent permitted under the applicable legislation, any limitations and/or exclusions of liability in the Agreement shall apply to this Annex I. In addition, the Processor shall only be liable under this Annex I if it has: (i) failed to comply with its specific obligations under the applicable Data Protection Legislation; or (ii) acted outside or in breach of the Controller's lawful instructions.

14.2. If, at any time during the Term, it is determined that any provision of this Annex I is or has become invalid, illegal, or unenforceable, the validity, legality, and enforceability of the remaining provisions of the Annex I shall not in any way be affected or impaired thereby. The Parties shall negotiate in good faith to replace such invalid, unlawful, or unenforceable provision with a valid, lawful and enforceable provision, the effect of which shall be as close as possible to that of the invalid, unlawful, or unenforceable provision.

14.3. This Annex I shall be governed by and construed in accordance with, the Billit Terms and Conditions (including the miscellaneous clauses), unless the context would require otherwise.

Schedule A – Description of processing and contact information

1. Purposes and specific instructions regarding the processing

☒ Business Purposes, including to provide the Billit Platform and the Services and to execute the Agreement, such as:

- to create, grant access to and login to the correct user accounts;
- for management of user accounts;
- to make use of the e-invoicing, billing and other functionalities available in the Platform: including:
  - collecting and storing Client's customer, vendor and transaction details in a digital format for e-invoicing;
  - generating, validating and sending e-invoices to Client recipients;
  - exchanging invoices with other systems or stakeholders upon the Client's request (e.g. accountants, clients, etc.);
- to integrate invoicing systems and software with the available e-invoicing networks (such as PEPPOL) (via the Billit e-invoicing access point PEPPOL) to send and receive e-invoices;
- to execute maintenance and support services;
- etc.

☐ Other (please specify): _____

2. Nature of the processing

☒ collection

☒ recording

☒ organization

☒ structuring

☒ storage

☒ adaptation or alteration

☒ retrieval

☒ consultation

☒ use

☒ disclosure by transmission, dissemination or otherwise making available

☒ alignment or combination

☒ restriction, erasure or destruction of data (whether or not by automated means)

☐ other (please specify): _____

3. Categories of Data Subjects

☒ (Potential/ex-) customers of Controller

☒ Applicants, (ex-) employees or interns of the Controller

☒ (Potential)/(ex) self-employed consultants of the Controller

☒ Users of the following service/website/application: the Billit Platform

☒ (Potential/ex-) suppliers of the Controller

☒ (Potential/ex-) business partners of the Controller

☐ Minors (below the age of 16)

☒ Other (please specify): all other individuals whose Personal Data is uploaded or otherwise available in the Platform.

4. Categories of Personal Data

☒ Personal identification data (*name, address, telephone number, etc.*)

☒ Electronic identification data (*IP address, MAC address, cookies, etc.*)

☐ Housing characteristics (*address, type of home, residence time, etc.*)

☐ Health related data (*physical health, mental health, genetic data, treatments, prescriptions, etc.*)

☒ Financial data (*bank account numbers, insurance, salary, invoicing data, including history of payments, payment balance, etc.*)

☐ Personal characteristic (*age, gender, date of birth, place of birth, citizenship, visas, etc.*)

☐ Psychological data (*opinions about personality, etc.*)

☐ Family (*marital status, cohabitation, name of spouse/partner, children, parents, etc.*)

☐ Memberships (*professional and non-professional memberships, clubs, groups, associations, etc.*)

☐ Judicial data (*data concerning convictions and offences, suspicions, indictments and administrative sanctions, etc.*)

☐ Financial and insurance products (*loans, mortgages, etc.)*

☐ Location data (*GPS, mobile phone or other tracking mechanisms, etc.)*

☐ Education (*curriculum, financing of studies, qualifications, professional experience, publications, etc.*)

☒ Profession and job (*current job, work description, job application data, career, salary, data concerning IT equipment, passwords and codes, etc.*)

☐ Lifestyle and (consumption) habits

☒ Account data (usernames, passwords and any other log-in data, etc.)

☐ Pictures or videos

☐ Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership

☐ Genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or sex life or sexual orientation

☐ Judicial data (*data concerning convictions and offences, suspicions, indictments and administrative sanctions, etc.*)

☒ All other categories of Personal Data uploaded in or generated by the usage of Processor's Platform and/or Services

☐ Other (please specify): _____

5. Retention period

☒ During the Term of the Agreement and as long as the Controller makes Personal Data available to the Processor in the context of the Agreement. For the avoidance of doubt, Billit is not obliged to retain data after the Term, unless as (i) required by applicable laws; (ii) required for Billit to perform any post-termination obligations; (ii) this Agreement otherwise states; or (iv) the Parties otherwise agree in writing;

☐ Specific retention periods, please specify: _____

6. Contact information for the person responsible for data protection compliance

	Processor
E-mail	dpo@billit.eu

7. List of Sub-Processors

The Controller has authorized the use of the Sub-Processors listed on https://www.billit.eu/en-int/subprocessors/ (as may be updated from time to time). Additionally, the Controller has authorize the following Sub-Processors:

Company name	**Type of sub-processing operation (description of services)**
Freelancers generally engaged in the execution of the Processor's daily activities (an updated list can be provided upon request)	Business Purposes
Affiliates	Business Purposes

8. Transfers of personal data

Category and location of recipients of Personal Data outside the EEA:

☒ Not applicable;

☐ Other (please specify): _____

Purpose(s) for transfer of Personal Data outside the EEA

☒ Not applicable;

☐ Other (please specify): _____

9. Technical and organizational measures

The Processor takes, at its own cost, appropriate technical and organizational measures to protect Personal Data, including, at a minimum, the following technical and organizational measures (non-exhaustive list):

- **Control of physical access**: Billit's web application, communication, and database servers are located in secure data centers in Europe, managed by Billit's hosting providers with which Billit has entered into the required written agreements as provided for in this Annex I.
- **Control of access to the system**: Billit has taken appropriate measures to prevent unauthorized persons from using its systems:
    - The identification of the terminal and/or the terminal's user in Billit's systems;
    - Automatic shut-down of the user terminal while not in use;
    - Identification and password required to regain access; The Controller can opt to activate MFA (Multi Factor Authentication) for end user accounts;
    - Automatic blocking of the user after repeated entry of a wrong password.
    - Registration and regular monitoring of events.
    - Access control via firewall, router, and VPN to protect the private networks and back-end servers.
    - Ad hoc monitoring of infrastructure security.
    - Regular inspections of security risks by internal staff and external auditors.
    - Issuing and safe keeping of identification codes.
    - Role-based access control according to the principle that only strictly necessary rights are granted.
    - Access to host servers, applications, databases, routers, switches, etc. is recorded.
    - The use of commercial and customized tools to collect and verify data recorded by the Platform and the system.
- **Control of access to data**: Billit has implemented appropriate measures to protect Personal Data against accidental destruction or loss:
    - Redundant infrastructure.
    - A constant evaluation of data centers and Internet Service Providers (ISPs) to optimize performance for clients in terms of bandwidth, latency, and isolation for disaster recovery.
    - Housing data centers in secure, carrier-neutral shared locations with physical security, redundant power supply, and redundant infrastructure.
- **Control of transfer**: Billit has implemented appropriate measures to prevent the reading, copying, modification, or erasure of Personal Data by unauthorized persons during data transmission or transport of the data carriers:
    - The use of appropriate firewall and encryption technologies to protect the ports and channels through which data is transferred.
    - Encryption of sensitive Personal Data during transmission using current versions of TLS or other security protocols that use strong encryption algorithms and keys.
    - Protection of employee access via the Internet to account management interfaces via encrypted TLS.
    - End-to-end encryption of shared screens for remote access, support, or real-time communication.

- **Control of the input**: Billit has implemented appropriate measures to ensure that it can be determined whether and by whom Personal Data has been entered into or deleted from the Personal Data Processing systems:
    - Authentication of the authorized employees.
    - Protective measures for the entry of Personal Data into the memory and the reading, modification, and erasure of stored Personal Data, including by documenting or logging significant changes to account details or settings.
    - Separation and protection of all stored Personal Data through database schedules, logic access controls, and/or encryption.
    - The use of proof of identity for user identification.
    - Physical security of the location where the data processing takes place.
    - Session time-out.
- **Data backups**.
- **Separation of data** by:
    - Individual allocation of System Administrators.
    - Taking appropriate measures to register the System Administrator's access to the infrastructure.

The Processor is committed to ensuring that personal data is protected at all levels - technical, physical, and organizational. The Processor's organizational measures and security practices are continuously reviewed and updated to address evolving threats and maintain a high level of data security and privacy. To continuously stay at pace with the evolving security standards, the Controller acknowledges and agrees that the measures described herein will be updated and amended from time to time (at Processor's sole discretion). Upon request, the Processor shall provide an updated version of this Schedule A.

Despite the above-mentioned measures, the Parties hereby acknowledge that there are always risks associated with sending personal data over the internet and that the security and protection of personal data can never be fully guaranteed, nor can it be guaranteed that unauthorized third parties will never be able to defeat those measures or use the personal data processed by Processor for improper purposes.

Any authorized Sub-processors shall implement *mutatis mutandis* the technical and organizational measures as defined in this Schedule A or such other measures resulting in an equivalent or higher level of protection of personal data as deemed useful or necessary by such sub-processors. Upon request, the Client can request the Processor to provide the latest version of the implemented technical and organizational measures by said Sub-processors.