iTraceiT

Data Processing Agreement

GDPR Article 28 — Processor Agreement

Version	v1.1
Date	November 2026
Effective date	1 November 2026
Governing law	Belgian law
Jurisdiction	Court of Nivelles (Brabant Wallon)
Language	English

iTraceiT srl | Rue de Rodeuhaie 4, 1348 Louvain-la-Neuve, Belgium | BE 0770.300.358

PREAMBLE

This Data Processing Agreement ("DPA") is entered into between iTraceiT srl (the "Processor") and the Customer identified in the applicable Order Form (the "Controller"). It governs all processing of Personal Data carried out by iTraceiT on behalf of the Customer in connection with the Services, in accordance with Article 28 of Regulation (EU) 2016/679 (GDPR).

This DPA is incorporated by reference into the Agreement and forms a non-overridable part thereof. In the event of any conflict between this DPA and any other document forming part of the Agreement, this DPA prevails with respect to data protection matters.

Article 1 — Definitions

Terms defined in the GTC have the same meaning in this DPA. In addition:

Controller: the Customer, who determines the purposes and means of the processing of Personal Data.

Processor: iTraceiT srl, who processes Personal Data on behalf of the Controller.

Processing / Process: any operation or set of operations performed on Personal Data, as defined in the GDPR.

Sub-processor: any third party engaged by iTraceiT to process Personal Data in the course of providing the Services.

Data Subject: an identified or identifiable natural person whose Personal Data is processed under this DPA.

Personal Data Breach: a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data.

Article 2 — Subject Matter, Nature, and Purpose of Processing

2.1 iTraceiT processes Personal Data solely in order to provide the Services described in the Agreement — specifically, to operate, maintain, and improve the iTraceiT Platform for the benefit of the Controller. Processing is carried out on the documented instructions of the Controller, as expressed through the Agreement and the Controller's use of the Platform.

2.2 The nature of the processing includes: storage, retrieval, display, structuring, transmission, consultation, use, and deletion of Personal Data through the Platform.

2.3 iTraceiT will not process Personal Data for any other purpose, including its own commercial or marketing purposes, unless required to do so by applicable Union or Member State law, in which case iTraceiT will inform the Controller before processing unless prohibited by law.

Article 3 — Duration of Processing

3.1 Processing of Personal Data begins on the Effective Date and continues for the duration of the Agreement. Upon expiry or termination, iTraceiT will continue to hold Personal Data for a period of thirty (30) days to enable data export by the Controller, unless a longer retention period is required by applicable law.

3.2 After the period referred to in Article 3.1, iTraceiT will securely and permanently delete or anonymise all Personal Data, unless it is required by applicable law to retain specific data, in which case it will notify the Controller accordingly.

Article 4 — Categories of Personal Data and Data Subjects

4.1 The categories of Personal Data processed under this DPA are determined by the Controller and may include:

Contact information: names, professional email addresses, telephone numbers, job titles, employer names.

Authentication data: usernames and hashed/encrypted passwords.

Operational and traceability data: product identifiers, batch references, supply chain transaction records, timestamps, QR code data, blockchain export records.

Communication data: support ticket content, email exchanges between users and iTraceiT support.

Technical data: IP addresses, browser type, session identifiers, and access logs, to the extent these constitute Personal Data.

4.2 The categories of Data Subjects whose Personal Data may be processed include:

Employees, agents, and contractors of the Controller who are granted access to the Platform.

Supply chain partners, suppliers, and sub-contractors of the Controller whose contact information is entered into the Platform.

End consumers, to the extent the Controller uses consumer-facing Digital Product Passport features of the Platform.

Article 5 — Obligations of the Processor

5.1 Instructions: iTraceiT processes Personal Data only on the documented instructions of the Controller. The Agreement and the Controller's configuration and use of the Platform constitute such instructions. If iTraceiT is required by Union or Member State law to process Personal Data for another purpose, it will inform the Controller in advance, unless prohibited by law.

5.2 Confidentiality: iTraceiT ensures that all personnel authorised to process Personal Data are bound by appropriate contractual or statutory obligations of confidentiality.

5.3 Security: iTraceiT implements and maintains appropriate technical and organisational measures to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access, as described in Article 9.

5.4 Sub-processors: iTraceiT engages Sub-processors only in accordance with Article 6. iTraceiT remains fully liable to the Controller for the performance of Sub-processors' obligations under this DPA.

5.5 Data Subject Rights: iTraceiT assists the Controller, by appropriate technical and organisational measures and to the extent reasonably possible, in fulfilling the Controller's obligations to respond to Data Subject rights requests under Chapter III of the GDPR (access, rectification, erasure, restriction, portability, objection). iTraceiT will promptly forward any Data Subject requests it receives directly to the Controller.

5.6 Assistance with Obligations: iTraceiT assists the Controller in ensuring compliance with the obligations under Articles 32 to 36 of the GDPR (security, data breach notification, data protection impact assessment, prior consultation), taking into account the nature of the processing and the information available to iTraceiT.

5.7 Deletion or Return: At the choice of the Controller, iTraceiT will delete or return all Personal Data following expiry or termination of the Agreement, in accordance with Article 3, and will delete existing copies unless applicable law requires their retention.

5.8 Information and Audit: iTraceiT makes available to the Controller all information necessary to demonstrate compliance with the obligations under this DPA, and allows for and contributes to audits and inspections in accordance with Article 10.

5.9 Blockchain Exports: Data that the Controller decides to export to the blockchain is published and becomes definitive after the short cancellation period indicated in the Platform; it can then no longer be rectified or erased. The Controller shall not instruct the export of Personal Data to the blockchain. iTraceiT's obligations of rectification, erasure and return under this DPA do not extend to data exported to the blockchain in breach of this Article.

Article 6 — Sub-processors

6.1 The Controller grants iTraceiT general written authorisation to engage Sub-processors to assist in the provision of the Services. The current list of Sub-processors, including their location and the transfer safeguards applied, is published and maintained at itraceit.io/sub-processors.

6.2 iTraceiT gives the Controller at least thirty (30) days' prior written notice of any intended addition or replacement of Sub-processors. The Controller may object to a new or replacement Sub-processor within fifteen (15) days of such notice on reasonable, documented grounds relating to data protection. Where the Controller objects and iTraceiT cannot accommodate the objection, either Party may terminate the relevant Services on thirty (30) days' notice without penalty.

6.3 iTraceiT imposes on all Sub-processors data protection obligations equivalent to those set out in this DPA by way of a written contract. iTraceiT remains fully liable to the Controller for the performance of Sub-processors.

Article 7 — International Transfers

7.1 iTraceiT hosts Personal Data within the European Economic Area ("EEA"), in the AWS Frankfurt region (eu-central-1), with copies of monthly backups in the AWS Ireland region (eu-west-1).

7.2 The Controller acknowledges that members of iTraceiT's team located in Sri Lanka and, where applicable, iTraceiT's local partners providing support outside the EEA may access Personal Data remotely, only on iTraceiT's prior authorisation, on a need-to-know basis and to the extent necessary for the support, maintenance or development of the Services. Such access constitutes a transfer of Personal Data to a third country. Where the country concerned, such as Sri Lanka, is not covered by an adequacy decision of the European Commission, iTraceiT ensures that each such

transfer is governed by the Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914 (Module 3, processor to processor, or Module 2 where applicable), supported by a transfer impact assessment and supplementary measures, including individual accounts with multi-factor authentication, logging of access, encryption in transit, and no local storage or download of Customer Data except where strictly necessary.

7.3 Where processing by any other Sub-processor involves a transfer of Personal Data outside the EEA, iTraceiT ensures that the transfer is subject to appropriate safeguards in accordance with Chapter V of the GDPR.

7.4 iTraceiT will inform the Controller of any new transfer of Personal Data outside the EEA in accordance with Article 6.2 and provide a copy of the relevant safeguards on request; commercial terms may be redacted.

Article 8 — Personal Data Breach Notification

8.1 iTraceiT notifies the Controller without undue delay and, where feasible, within seventy-two (72) hours of becoming aware of a Personal Data Breach affecting Personal Data processed under this DPA.

8.2 The notification will include, to the extent available at the time: (a) a description of the nature of the breach, including the categories and approximate number of Data Subjects and Personal Data records affected; (b) the name and contact details of the DPO; (c) a description of the likely consequences of the breach; and (d) a description of the measures taken or proposed to address the breach, including mitigation measures.

8.3 Where all required information cannot be provided in the initial notification, iTraceiT will provide it in further communications as soon as it becomes available.

8.4 iTraceiT will cooperate fully with the Controller in notifying the competent supervisory authority and, where required, the affected Data Subjects.

Article 9 — Technical and Organisational Security Measures

9.1 iTraceiT implements and maintains technical and organisational measures appropriate to the risk, including at a minimum:

Encryption of Personal Data in transit using TLS 1.2 or higher, and at rest using AES-256 or equivalent.

Role-based access controls ensuring that Personal Data is accessible only to personnel with a legitimate need.

Multi-factor authentication options for administrative access to the Platform infrastructure.

Automated daily backups, retained for a few days, and monthly backups, retained for ninety (90) days, stored in the AWS Frankfurt region (eu-central-1); monthly backups are additionally copied to the AWS Ireland region (eu-west-1), within the EEA; daily backups are not copied to another region; restoration is tested automatically every month.

Comprehensive audit logging of access to and modifications of Personal Data.

Vulnerability management and security patch procedures.

An incident response plan covering detection, containment, investigation, and notification of security incidents.

Physical and environmental security controls at hosting facilities operated by certified Sub-processors.

9.2 iTraceiT reviews and updates its security measures at regular intervals and in response to changes in the threat landscape. The Controller acknowledges that no security measures can provide absolute protection and that iTraceiT's obligation is one of appropriate means, not of guaranteed results.

Article 10 — Audit Rights

10.1 Upon the Controller's written request, iTraceiT will make available all information reasonably necessary to demonstrate compliance with this DPA. iTraceiT may first satisfy such a request by providing a completed data protection questionnaire, third-party audit report, or equivalent documentation.

10.2 Where the Controller reasonably determines that such documentation is insufficient, the Controller may, no more than once per calendar year and on at least thirty (30) days' prior written notice, conduct or commission an on-site audit of iTraceiT's processing activities. The audit must be conducted during normal business hours, in a manner that minimises disruption to iTraceiT's operations, and at the Controller's expense.

10.3 iTraceiT may refuse access to information that it reasonably considers commercially sensitive, provided it can demonstrate by other means that the relevant obligations are being met.

Article 11 — Data Protection Officer

11.1 iTraceiT has designated a Data Protection Officer who can be contacted at: Guy De Smet — guy@itraceit.io.

11.2 The Controller may contact iTraceiT's DPO at any time on matters relating to data protection and this DPA.

Article 12 — Liability and Governing Law

12.1 Each Party's liability under this DPA is subject to the limitations set out in Article 11 of the GTC, except where mandatory GDPR provisions impose liability that cannot be limited by contract.

12.2 This DPA is governed by Belgian law. Any dispute arising out of or in connection with this DPA that the Parties cannot resolve by good-faith negotiation shall be submitted to the exclusive jurisdiction of the competent courts of Nivelles (Brabant Wallon), Belgium.

Version 1.1 — November 2026 (effective 1 November 2026) | iTraceiT srl | Rue de Rodeuhaie 4, 1348 Louvain-la-Neuve, Belgium | itraceit.io/dpa