

InformaIT Data Processing

Addendum

Version 2026.1 | Effective 21 October 2026

1. Introduction and scope

1.1 This Data Processing Addendum ("DPA") forms part of the Subscription Contract, SaaS Agreement or other agreement for InformaIT's hosted software products and related support services (the "Main Agreement") between InformaIT AB, org. no. 556615-0610, Hamngatan 4, 211 22 Malmö, Sweden ("InformaIT") and the customer that has entered into the Main Agreement ("Customer"). InformaIT and Customer are each a "Party".

1.2 This DPA applies to the extent InformaIT processes Customer Personal Data on behalf of Customer in providing the Services, and Data Protection Law applies to that processing.

1.3 This DPA does not apply to Personal Data that InformaIT processes as a controller (clause 5), or to on-premise installations of the Products, except where InformaIT accesses Customer Personal Data while providing support for such an installation.

1.4 For the subject matter of data protection, the order of precedence is: (a) the Standard Contractual Clauses, where they apply under clause 10; (b) this DPA; (c) the Main Agreement. Nothing in the Main Agreement limits a Data Subject's rights under the Standard Contractual Clauses.

1.5 Capitalized terms not defined in this DPA have the meaning given in the Main Agreement. Customer accepts this DPA by entering into the Main Agreement; no separate signature is required, but InformaIT will countersign a copy on request.

2. Definitions

"Affiliate" means an entity that controls, is controlled by, or is under common control with a Party.

"Customer Personal Data" means Personal Data that InformaIT processes on behalf of Customer under the Main Agreement, as described in Schedule 1.

"Data Protection Law" means all laws applicable to the processing of Customer Personal Data under this DPA, as amended or replaced, including: Regulation (EU) 2016/679 ("GDPR") and EU Member State laws supplementing it; the GDPR as it forms part of the law of the United Kingdom and the UK Data Protection Act 2018 (together "UK GDPR"); the Swiss Federal Act on Data Protection ("FADP"); Directive 2002/58/EC as implemented; US State Privacy Laws; and other applicable laws such as Brazil's LGPD, Singapore's PDPA 2012, Australia's Privacy Act 1988 and Canada's PIPEDA.

"EEA" means the European Economic Area: the Member States of the European Union together with Iceland, Liechtenstein and Norway.

"Personal Data", "Controller", "Processor", "Data Subject", "Processing" and "Supervisory Authority" have the meanings given in the GDPR. They include the equivalent terms under other Data Protection Law, such as "business", "service provider" and "consumer" under US State Privacy Laws and "organization", "data intermediary" and "individual" under the PDPA.

"Products" and **"Services"** have the meanings given in the Main Agreement.

"Restricted Transfer" means storing, processing or accessing Customer Personal Data in a country outside the EEA, the United Kingdom or Switzerland that is not covered by an adequacy decision of the relevant authority. Remote access from such a country is a Restricted Transfer even where no copy is made.

"Security Incident" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data. It does not include unsuccessful attempts or activities that do not compromise the security of Customer Personal Data, such as unsuccessful log-in attempts, port scans or denial-of-service attacks that do not result in access.

"Standard Contractual Clauses" or "SCCs" means the standard contractual clauses in Commission Implementing Decision (EU) 2021/914, Module Two (controller to

processor) and Module Three (processor to processor), with the elections in Schedule 4.

"Sub-processor" means any third party, including an InformaIT Affiliate, engaged by InformaIT to process Customer Personal Data.

"Sub-processor List" means the list of Sub-processors published on the Trust Center at <https://informait.com/trust>, as updated in accordance with clause 9.

"Swiss Amendments" means the modifications to the SCCs set out in Schedule 4, Part C, required by the Swiss Federal Data Protection and Information Commissioner for transfers subject to the FADP.

"Trust Center" means InformaIT's public security and privacy page at <https://informait.com/trust>, where the Sub-processor List, change notices, the current description of technical and organizational measures and the current version of this DPA are published.

"UK Addendum" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner under section 119A of the Data Protection Act 2018, version B1.0, in force from 21 March 2022.

"US State Privacy Laws" means the California Consumer Privacy Act as amended by the California Privacy Rights Act ("CCPA"), and any other US state law regulating the processing of consumers' personal data that applies to the Processing of Customer Personal Data, together with their regulations.

3. Roles of the Parties

3.1 Customer is the Controller of Customer Personal Data, or a Processor acting on behalf of a third-party Controller. InformaIT is a Processor, or a Sub-processor where Customer is a Processor. Under US State Privacy Laws, Customer is the business or controller and InformaIT is the service provider or processor.

3.2 Where Customer acts as a Processor, Customer warrants that the relevant Controller has authorized Customer's instructions, the appointment of InformaIT as Sub-processor and, where applicable, the conclusion of the SCCs (Module Three).

3.3 Customer is responsible for: (a) the lawfulness of Customer Personal Data and of its instructions; (b) providing notices to, and obtaining any legal basis from, Data Subjects; (c) deciding which data it uploads to the Products and configuring users, roles, access and retention in the Products; (d) not uploading Personal Data in documents, artwork or other content, beyond business contact details that incidentally appear in them, and never special categories of Personal Data, unless agreed with InformaIT in writing; InformaIT does not monitor the content of uploaded files; and (e) keeping its administrative and security contact details, as registered in the Products, the Main Agreement or as otherwise notified to InformaIT in writing, current, since InformaIT sends notices under this DPA to those contacts.

3.4 Customer's Affiliates that use the Services under the Main Agreement are covered by this DPA. Customer enters into this DPA on their behalf, exercises their rights under it, and is responsible for their compliance with it.

4. Processing instructions and purpose

4.1 InformaIT processes Customer Personal Data only on Customer's documented instructions. Customer's complete instructions are: (a) the Main Agreement and this DPA; (b) Customer's use and configuration of the Products; and (c) other written instructions agreed between the Parties. InformaIT may also process Customer Personal Data where required by EU or Member State law to which InformaIT is subject; in that case InformaIT informs Customer of the legal requirement before processing, unless the law prohibits this on important grounds of public interest.

4.2 The purpose of the processing is to provide, maintain, secure and support the Services. The subject matter, duration, nature of the processing, types of Personal Data and categories of Data Subjects are set out in Schedule 1.

4.3 If InformaIT considers that an instruction infringes Data Protection Law, it informs Customer without undue delay and may suspend performance of that instruction until the Parties have agreed how to proceed.

4.4 Instructions that go beyond the scope of the Main Agreement require prior written agreement, which may include additional fees.

4.5 InformaIT does not: (a) sell or share Customer Personal Data; (b) use Customer Personal Data for its own purposes, except as set out in clause 5; (c) use Customer Personal Data to train or improve machine-learning models; or (d) combine Customer Personal Data with Personal Data from other sources, except as necessary to provide the Services.

5. InformaIT as controller

5.1 InformaIT is an independent Controller of: (a) business contact and account data of Customer's personnel, which it processes for contract management, billing, support communications, service notices, security, fraud prevention and the establishment, exercise or defense of legal claims; and (b) usage and performance data about the Products that has been aggregated or anonymized so that it is no longer Personal Data. This processing is governed by InformaIT's privacy policy at <https://informait.com/trust#privacy-policy>, not by this DPA.

5.2 Nothing in this DPA restricts the processing in clause 5.1, provided it complies with Data Protection Law and with the confidentiality obligations in the Main Agreement.

6. Confidentiality and personnel

6.1 InformaIT ensures that persons authorized to process Customer Personal Data are bound by contractual or statutory obligations of confidentiality, have received security and data protection training, and have access only to the Customer Personal Data they need for their role.

6.2 InformaIT takes reasonable steps to ensure the reliability of its personnel and removes access promptly when a person's role no longer requires it or their engagement ends.

7. Security measures

7.1 InformaIT implements and maintains the technical and organizational measures described in Schedule 2, and such further measures as are appropriate to the risk, to protect Customer Personal Data against Security Incidents and to meet the requirements of Article 32 GDPR.

7.2 InformaIT maintains an information security management system certified to ISO/IEC 27001 that covers the Services, and makes the current certificate available on the Trust Center or on request.

7.3 InformaIT may update the measures in Schedule 2 as technology and threats develop, provided the updates do not materially reduce the overall level of security of the Services. InformaIT publishes material changes on the Trust Center and emails Customer's registered contacts at least 30 days before the change takes effect, except where a shorter period is needed to address a security risk.

7.4 Customer is responsible for the secure use of the Products on its side, including managing its users and roles, protecting credentials, configuring single sign-on and multi-factor authentication where offered, and deciding what data it uploads.

8. Security incidents

8.1 InformaIT notifies Customer of a Security Incident without undue delay and in any event within 48 hours after becoming aware of it, by email to Customer's registered security contact.

8.2 The notification describes, to the extent known: the nature of the Security Incident; the categories and approximate number of Data Subjects and records concerned; the likely consequences; the measures taken or proposed to address it; and a point of contact at InformaIT. Where this information is not available at once, InformaIT provides it in phases without undue further delay.

8.3 InformaIT provides reasonable assistance to Customer in meeting Customer's obligations to notify Supervisory Authorities and Data Subjects. InformaIT does not notify Supervisory Authorities or Data Subjects of a Security Incident on Customer's behalf unless Customer instructs it to or the law requires it.

8.4 A notification under this clause is not an acknowledgement of fault or liability.

8.5 InformaIT documents Security Incidents, their effects and the remedial action taken, and makes this documentation available to Customer on request as far as it concerns Customer Personal Data.

9. Sub-processors

9.1 Customer gives InformaIT general written authorization to engage Sub-processors. The Sub-processors engaged at the date of the Main Agreement are those on the Sub-processor List at that date. For each Sub-processor, the Sub-processor List states the legal entity, the service it performs, the categories of Customer Personal Data it processes, the countries or regions where the data is stored or accessed, and the transfer mechanism relied on.

9.2 Before a new or replacement Sub-processor processes Customer Personal Data, InformaIT publishes the change on the Sub-processor List and notifies Customer's registered contacts by email at least 30 days in advance. Customer may also subscribe to change notifications on the Trust Center. The notice period runs from the date of the email.

9.3 Customer may object within the notice period on reasonable, documented grounds relating to data protection. The Parties then discuss the objection in good faith. InformaIT will, at its option, (a) not use the Sub-processor for Customer Personal Data, (b) propose a change to the Services or a different Sub-processor, or (c) if neither is commercially reasonable, inform Customer, who may then terminate the affected Services on written notice and receive a pro-rata refund of prepaid fees for the terminated Services. This is Customer's sole remedy for an objection.

9.4 InformaIT may replace a Sub-processor with less than 30 days' notice where this is necessary to maintain the security or continuity of the Services, in which case InformaIT notifies Customer as soon as practicable and Customer's objection right under clause 9.3 applies from that notice.

9.5 InformaIT engages each Sub-processor under a written contract that imposes data protection obligations no less protective than those in this DPA, including the requirements of Article 28(3) GDPR, and that provides for third-party beneficiary rights where the SCCs require them. On request, InformaIT provides Customer with the Sub-processor's published data processing terms or a copy of the relevant contract with commercial terms redacted.

9.6 InformaIT remains fully liable to Customer for the performance of each Sub-processor's data protection obligations.

9.7 Removal of a Sub-processor takes effect when published on the Sub-processor List and requires no advance notice.

10. International transfers

10.1 Hosting location. InformaIT stores and processes Customer Personal Data in the hosting region specified in the Main Agreement or otherwise agreed in writing. Where no region is specified, the region is the European Union. InformaIT does not move Customer Personal Data to a different region without Customer's written agreement, except for the Sub-processor processing disclosed on the Sub-processor List.

10.2 Transfers to InformaIT. InformaIT is established in Sweden. For Customers in the EEA, the United Kingdom and Switzerland, the disclosure of Customer Personal Data to InformaIT is not a Restricted Transfer. Customers in other jurisdictions are responsible for any requirement of their local Data Protection Law that applies to disclosing Personal Data to a processor in the EU, and InformaIT provides the information and cooperation reasonably needed to satisfy it.

10.3 Onward transfers by InformaIT. Where InformaIT, as exporter, makes a Restricted Transfer to a Sub-processor, including a Sub-processor in a hosting region chosen by Customer, InformaIT ensures before the transfer that one of the following applies, and records which on the Sub-processor List: (a) an adequacy decision of the European Commission, and of the UK or Swiss authorities where UK or Swiss Customer Personal Data is concerned; (b) for a recipient in the United States, the recipient's certification under the EU-U.S. Data Privacy Framework, including the UK Extension and the Swiss-U.S. Data Privacy Framework where relevant, which InformaIT verifies against the official list; or (c) the SCCs, Module Three, together with the UK Addendum and the Swiss Amendments where UK or Swiss Customer Personal Data is concerned, supported by a documented transfer impact assessment. InformaIT provides a summary of the relevant assessment on request.

10.4 Customer's authorization under clause 9.1 includes the onward transfers disclosed on the Sub-processor List. A change in a Sub-processor's location or transfer mechanism, other than a change of the hosting region under clause 10.1, is notified as a change under clause 9.2.

10.5 Fallback. If an adequacy decision relied on in clause 10.2 is suspended, invalidated or withdrawn so that a disclosure of Customer Personal Data to InformaIT becomes a Restricted Transfer, the Parties are deemed to have entered into the SCCs for that transfer, with Customer as data exporter and InformaIT as data importer,

Module Two where Customer is a Controller and Module Three where Customer is a Processor, with the elections in Schedule 4 and Schedules 1 and 2 as Annexes I and II. The UK Addendum and the Swiss Amendments apply to UK and Swiss Customer Personal Data respectively.

10.6 If a transfer mechanism relied on under this clause ceases to be valid, InformaIT suspends the affected transfer, informs Customer and either implements an alternative lawful mechanism or, where none is available within a reasonable period, allows Customer to terminate the affected Services with a pro-rata refund of prepaid fees.

11. Data subject rights and assistance

11.1 If InformaIT receives a request from a Data Subject concerning Customer Personal Data, it forwards the request to Customer within five business days and does not respond to the Data Subject except to refer them to Customer, unless the law requires otherwise. Customer is responsible for verifying the identity of the requester.

11.2 Customer's administrators create, deactivate and delete user accounts themselves in the Products' system console or through Customer's single sign-on provider. InformaIT exports other Customer Personal Data on Customer's written request within 10 business days in a common machine-readable format. Where a Data Subject request cannot be met in these ways, InformaIT provides reasonable assistance, taking into account the nature of the processing, at Customer's reasonable cost where the assistance goes beyond what is customary.

11.3 InformaIT provides reasonable assistance with data protection impact assessments and prior consultations with Supervisory Authorities, to the extent they concern the Services and the information is not already available on the Trust Center. Where such assistance involves material cost, the Parties agree the cost in advance.

11.4 InformaIT provides the information about the Services that Customer reasonably needs to maintain its records of processing activities.

12. Requests from public authorities and third parties

12.1 If InformaIT receives a legally binding request from a public authority or a third party for disclosure of Customer Personal Data, it: (a) notifies Customer promptly, unless legally prohibited; (b) where legally prohibited, uses reasonable efforts to obtain a waiver of the prohibition; (c) reviews the legality of the request and challenges it where there are reasonable grounds to do so; and (d) discloses only the minimum information required.

12.2 InformaIT does not disclose Customer Personal Data to public authorities voluntarily, and does not grant any public authority general or direct access to Customer Personal Data.

12.3 InformaIT keeps a record of requests received and the responses given, and makes the record available to Customer on request as far as it concerns Customer Personal Data.

13. Audits and compliance information

13.1 InformaIT makes available on the Trust Center or on request, under the confidentiality terms of the Main Agreement: its ISO/IEC 27001 certificate including the scope statement; the current description of its technical and organizational measures; the summary report of its annual independent penetration test; and completed industry-standard security questionnaires. Customer relies on this information in the first instance to verify InformaIT's compliance with this DPA.

13.2 Where the information in clause 13.1 is not sufficient to demonstrate compliance with Article 28 GDPR, Customer, or an independent auditor appointed by Customer and bound by confidentiality, may audit InformaIT's processing of Customer Personal Data: no more than once in any 12-month period; on at least 30 days' written notice; during normal business hours; with scope, duration and auditor agreed in advance; at Customer's cost; and in a manner that does not disrupt InformaIT's operations or compromise the security of other customers' data. Audits do not extend to the premises or systems of Sub-processors; for these, Customer relies on the Sub-processors' certifications and audit reports made available through InformaIT. Where the requested audit scope is covered by an ISO/IEC 27001 certificate or a third-party audit report issued within the preceding 12 months, and InformaIT confirms that there

has been no material change in the audited controls, Customer accepts that certificate or report in lieu of its own audit of those controls.

13.3 The limits in clause 13.2 on frequency and notice do not apply to an audit following a Security Incident affecting Customer Personal Data, or to an audit required by a Supervisory Authority.

13.4 Customer shares the audit findings with InformaIT. For material findings, InformaIT provides a remediation plan within 30 days. InformaIT may charge its reasonable costs for audits that exceed two person-days of its staff time, except where the audit reveals material non-compliance.

14. Return and deletion

14.1 During the term, Customer deletes user accounts itself as described in clause 11.2. InformaIT deletes or anonymizes other Customer Personal Data on Customer's written request within 30 days. Audit trail records are retained for the period Customer specifies to meet its regulatory record-keeping obligations; erasure requests concerning them are met by anonymizing the user reference. Deletion from backups follows clause 14.2.

14.2 After expiry or termination of the Main Agreement, Customer may export Customer Personal Data for 30 days. InformaIT then deletes Customer's instance, including its databases and storage, within 90 days after termination, unless EU or Member State law requires InformaIT to retain specific data. Backups are protected by a retention policy that prevents earlier deletion and expire automatically within the backup retention period stated on the Trust Center, which does not exceed 60 days, so all backup copies are gone no later than that period after the instance is deleted. On request, InformaIT confirms deletion in writing.

14.3 Customer Personal Data retained under this clause remains subject to this DPA and is processed only for the purpose of the retention.

15. Jurisdiction-specific terms

15.1 United Kingdom. For Customer Personal Data subject to UK GDPR: references to the GDPR and to a Supervisory Authority are read as references to UK GDPR and to

the Information Commissioner; the UK Addendum applies to any Restricted Transfer made under the SCCs, with the tables completed as in Schedule 4, Part B; and the UK adequacy regulations for the EEA apply to the disclosure of Customer Personal Data to InformaIT.

15.2 Switzerland. For Customer Personal Data subject to the FADP: references to the GDPR are read as references to the FADP where the FADP applies; the Swiss Federal Data Protection and Information Commissioner is the competent authority; the Swiss Amendments in Schedule 4, Part C apply to any Restricted Transfer made under the SCCs; and Switzerland's recognition of EU and EEA states as providing adequate protection applies to the disclosure of Customer Personal Data to InformaIT.

15.3 United States. For Customer Personal Data subject to US State Privacy Laws, InformaIT acts as a service provider or processor and: (a) does not sell or share Customer Personal Data; (b) does not retain, use or disclose Customer Personal Data for any purpose, including a commercial purpose, other than the business purposes specified in the Main Agreement, or outside the direct business relationship between the Parties; (c) does not combine Customer Personal Data with Personal Data it receives from other sources, except as permitted by US State Privacy Laws; (d) complies with the obligations applicable to service providers and processors and provides the same level of privacy protection as those laws require of Customer; (e) notifies Customer if it determines it can no longer meet its obligations under US State Privacy Laws; (f) grants Customer the right, on reasonable notice, to take reasonable and appropriate steps to stop and remediate unauthorized use of Customer Personal Data, and to verify InformaIT's compliance through the audit rights in clause 13; and (g) does not attempt to re-identify de-identified data received from Customer. InformaIT certifies that it understands and will comply with these restrictions. InformaIT does not accept protected health information under HIPAA and does not enter into business associate agreements; Customer must not upload such information to the Products.

15.4 Other jurisdictions. Where Customer's local Data Protection Law, including Brazil's LGPD, Singapore's PDPA, Australia's Privacy Act or Canada's PIPEDA, requires terms for the engagement of a processor or for the disclosure of Personal Data to a processor in the EU that are not contained in this DPA, the Parties cooperate in good faith to agree a short local-law addendum. Until then, InformaIT's obligations under

this DPA are read to include the equivalent obligations of a processor, data intermediary or operator under that law, to the extent compatible with this DPA.

16. General

16.1 Liability. Each Party's liability under this DPA is subject to the exclusions and limitations of liability in the Main Agreement, and the limits there apply in aggregate to claims under the Main Agreement and this DPA together. This clause does not limit a Party's liability to Data Subjects under the SCCs or a liability that cannot be limited under Data Protection Law.

16.2 Term. This DPA applies for as long as InformaIT processes Customer Personal Data, including the retention periods in clause 14.

16.3 Changes. InformaIT may amend this DPA: (a) where required by a change in Data Protection Law, a decision of a Supervisory Authority or a court, or a change to the SCCs or UK Addendum; or (b) to update the Trust Center addresses and other references that do not change the Parties' obligations. For an amendment under (a) that would materially reduce Customer's protections, InformaIT publishes the change on the Trust Center and emails Customer's registered contacts at least 30 days before it takes effect, or such shorter period as the law requires. Other changes require written agreement.

16.4 Notices. Notices from InformaIT under this DPA are sent by email to the administrative and security contacts Customer has registered in the Products, the Main Agreement or as otherwise notified to InformaIT in writing. Notices to InformaIT are given through the InformaIT customer portal at <https://support.portal.informait.com> or by email to privacy@informait.com. Both create a ticket in InformaIT's support system, and the ticket timestamp is the time of receipt.

16.5 Governing law. This DPA is governed by the law that governs the Main Agreement, except that the SCCs are governed by the law and subject to the courts chosen in Schedule 4. If the Main Agreement is governed by the law of a country outside the EEA, this DPA is governed by the laws of Sweden.

16.6 Severability. If a provision of this DPA is held invalid, the remaining provisions remain in force and the Parties replace the invalid provision with a valid one that comes closest to its purpose.

16.7 Language. This DPA is concluded in English. A translation is provided for convenience only.

Schedule 1 – Description of processing

This Schedule is also Annex I to the SCCs where they apply under clause 10.

A. Parties

	Data exporter	Data importer
Name	Customer, as identified in the Main Agreement	InformalT AB, org. no. 556615-0610
Address	As in the Main Agreement	Hamngatan 4, 211 22 Malmö, Sweden
Contact	Customer's registered privacy or administrative contact	privacy@informait.com
Role	Controller (Module Two) or Processor (Module Three)	Processor, or Sub-processor where Customer is a Processor
Activities	Use of the Services for the proofreading, comparison and approval of documents, artwork and other content	Provision, hosting, maintenance and support of the Services

B. Description of the processing

Item	Description
Categories of Data Subjects	Customer's authorized users of the Products (employees, contractors, agency staff); individuals whose business contact details incidentally appear in documents, artwork and files uploaded by Customer, such as authors and approvers; Customer personnel who contact InformalT support; recipients of service communications designated by Customer
Categories of Personal Data	Identification and contact data (name, business email, username, job role); authentication data (hashed passwords for local accounts, or identity-provider identifiers where the customer uses single

Item	Description
	sign-on); activity and audit-trail data (actions in the Products with username or email and timestamp; IP address in certain audit records and system logs); content data: the Products are not intended for Personal Data in uploaded content, Customer is to upload none beyond business contact details that incidentally appear in documents and artwork, and InformaIT does not monitor content; support data: ticket content and attachments
Special categories	None intended. Customer must not upload special categories of Personal Data unless agreed in writing. Where uploaded content incidentally contains such data, Customer is responsible for the lawfulness of the processing, and InformaIT applies the measures in Schedule 2
Frequency	Continuous during the term of the Main Agreement
Nature of the processing	Hosting, storage, comparison and analysis of uploaded content, display to authorized users, transmission of results and notifications, backup, deletion; access by support personnel on Customer's request
Purpose	Provision, maintenance, security and support of the Services under the Main Agreement
Duration and retention	Term of the Main Agreement, then deletion in accordance with clause 14
Transfers to Sub-processors	As set out on the Sub-processor List, including subject matter, nature, duration and transfer mechanism for each Sub-processor

C. Competent supervisory authority

Exporter	Authority
Established in an EEA state	The supervisory authority of that state, per Clause 13 of the SCCs
Not established in the EEA but subject to GDPR	The supervisory authority of the EEA state where the exporter's Article 27 representative is established, or where the Data Subjects are
United Kingdom	Information Commissioner's Office

Exporter	Authority
Switzerland	Federal Data Protection and Information Commissioner

InformalT's lead supervisory authority is Integritetsskyddsmyndigheten (IMY), Sweden.

Schedule 2 – Technical and organizational measures

This Schedule is also Annex II to the SCCs where they apply. It describes the measures in place at the date of the Main Agreement; the current description is maintained on the Trust Center and updated under clause 7.3.

Area	Measures
Governance	Information security management system certified to ISO/IEC 27001:2022; appointed Security Officer and Privacy Officer; annual risk assessment, internal audit and management review; documented policies covering access, suppliers, secure development, incidents and business continuity
Personnel	Confidentiality undertakings for all staff and contractors; security awareness training at onboarding and at least annually; access rights removed on role change or departure
Access control	Single sign-on with multi-factor authentication for InformalT staff; role-based access on a least-privilege basis; privileged access limited to named operations staff and reviewed twice a year; customer-managed users and roles in the Products, with local accounts or single sign-on through the customer's identity provider
Tenant isolation	One dedicated instance per customer (single-tenant); customer environments logically separated; hosting region per the Main Agreement
Encryption	TLS 1.2 or higher for data in transit; encryption at rest for storage and backups using the cloud provider's default managed keys
Vulnerability management	Automated scanning of source code, dependencies and cloud configuration in the development pipeline;

Area	Measures
	remediation prioritized by severity; annual independent penetration testing, with the summary report available to customers on request
Logging and monitoring	Cloud audit logs retained in locked, tamper-protected storage for the retention period stated on the Trust Center; application logs kept within the customer's instance and deleted with it at offboarding; audit trail of user and administrator actions in the Products; alerting on security-relevant events
Backup and continuity	Regular encrypted backups kept in the customer's hosting region for the retention period stated on the Trust Center, protected against early deletion by a retention policy; periodic restore testing; business continuity and disaster recovery plan with defined recovery time and recovery point objectives, stated on the Trust Center
Secure development	Secure development policy; code review before merge; separated development, test and production environments; change management and validation in line with GAMP 5
Incident management	Documented incident response procedure; classification, containment, root-cause analysis and lessons learned; customer notification within 48 hours under clause 8
Supplier management	Supplier policy; data processing agreements and security requirements for all Sub-processors; periodic review of supplier certifications and performance indicators
Physical security	Production systems hosted in cloud data centers certified to ISO/IEC 27001 and SOC 2; Malmö office with controlled entry and clean-desk rules; remote working on managed devices under InformaIT's endpoint device policy and code of conduct
Data deletion	Deletion of customer data at termination per clause 14; secure disposal of storage media handled by the cloud provider under its certifications
Assistance to the Controller	Customer-managed user lifecycle via system console or single sign-on; export and deletion of other data on request within defined timeframes; support procedures for data subject requests; this Schedule, the ISO 27001 certificate and

Area	Measures
	questionnaire responses available via the Trust Center

Schedule 3 – Sub-processors

The Sub-processors authorized at the date of the Main Agreement are those published on the Trust Center at <https://informait.com/trust> on that date. The list states, for each Sub-processor, the legal entity, the service performed, the categories of Customer Personal Data processed, the countries or regions of storage and access, the transfer mechanism, and, where published, a link to the Sub-processor's own data processing terms and sub-processor list. Changes are made under clause 9 and recorded in the change log on that page. Where the SCCs apply under clause 10.5, this Schedule is Annex III.

Schedule 4 – Standard Contractual Clauses elections

Part A – EU SCCs (Decision 2021/914)

Clause	Election
Module	Module Two where Customer is a Controller; Module Three where Customer is a Processor
Clause 7 (docking)	Not applicable
Clause 9(a)	Option 2, general written authorization. The time period is 30 days, as in clause 9.2 of this DPA
Clause 11(a)	The optional independent dispute resolution body is not selected
Clause 13	The competent supervisory authority is determined per Schedule 1, Part C
Clause 17	Option 1. The Clauses are governed by the laws of Sweden
Clause 18(b)	The courts of Sweden
Annex I	Schedule 1
Annex II	Schedule 2

Clause	Election
Annex III	Schedule 3 (the Sub-processor List)

Part B – UK Addendum

Table	Completion
Table 1 (Parties)	As in Schedule 1, Part A
Table 2 (Selected SCCs)	The Approved EU SCCs, with the module and elections in Part A above, including the Appendix information
Table 3 (Appendix information)	Annex 1A and 1B: Schedule 1; Annex II: Schedule 2; list of Sub-processors: Schedule 3
Table 4 (Ending the Addendum)	Either Party may end the Addendum as set out in section 19

Part C – Swiss Amendments

For transfers subject to the FADP, the SCCs are read with these changes: references to the GDPR are read as references to the FADP; references to EU Member States include Switzerland, so that Swiss Data Subjects may bring claims in Switzerland; the Federal Data Protection and Information Commissioner is the competent supervisory authority under Clause 13, and acts in parallel with the EU authority where a transfer is subject to both the GDPR and the FADP.