Ascertia Data Processing Addendum

Effective starting: 6 March 2026

This Data Processing Addendum ("DPA") supplements the Ascertia Software License Agreement, applicable terms of use, or any other agreement governing the Customer's use of Ascertia's Products and any associated Support and Advisory Services (together, the "Agreement") entered into between the Customer and Ascertia. Except where expressly defined in this DPA or in the Agreement, any capitalised terms used in this DPA shall have the meanings assigned to them in Section 9 of this DPA.

1. Scope and Terms

1.1 Roles of the Parties

For the purposes of the Agreement, the Parties acknowledge and agree as follows:

(a) **Customer** refers to the legal entity that has entered into the Agreement with Ascertia which either: (i) acts as the controller of Customer Data; or (ii) processes Customer Data as a Processor on behalf of another Customer, including, where applicable, its Affiliates and/or its own customers (for example, where the Customer operates as a distributer, reseller, or other commercial partner).

(b) **Customer End User** or **End Customer** means a third party for whom the Customer processes Customer Data, including customers of the Customer acting as a reseller, distributor, or other commercial intermediary.

(c) The Customer acts either as a **Controller** in respect of Customer Data, or as a **Processor** processing Customer Data on behalf of another Customer (such as an Affiliate), and in such cases is responsible for providing Ascertia with the applicable processing instructions. Further details of the processing activities are set out in Schedule 1 (Description of Processing).

(d) Ascertia processes Customer Data solely as a Processor or, where applicable, as a Sub-processor. The nature and scope of such processing are described in Schedule 1 (Description of Processing).

1.2 Terms of this DPA

This DPA shall remain in effect for the duration of the Agreement and shall automatically end upon the expiry or earlier termination of the Agreement, or, where later, once Ascertia has ceased all Processing of Customer Personal Data.

1.3 Priority of Documents

In the event of any inconsistency or conflict between the documents forming part of the data processing framework, they shall apply in the following descending order of priority: (i) the applicable provisions set out in Schedule 2 (Region-Specific Terms, including any data transfer provisions); (ii) Schedule 1 (Description of Processing); (iii) Schedule 3 (Technical and Organisational measures); (iv) Schedule 4 (List of Sub-Processors); (v) the provisions of this DPA; and (vi) the Software License Agreement and Terms of Service and other contractual documentation.

2. Processing of Personal Data

2.1 Customer Instructions

(a) The Parties agree that this DPA, together with the Agreement, any applicable Orders, and the Customer's configuration, settings, and use of the Products and any related Support and Advisory Services, collectively set out the Customer's documented instructions governing Ascertia's Processing of Customer Data (the **"**Documented Instructions").

(b) Ascertia shall Process Customer Data only in accordance with the Documented Instructions, including as further described in Section 6.1 of Schedule 1. Without limiting the foregoing, the Customer:

(i) is responsible for ensuring that its Documented Instructions comply with all applicable Data Protection Laws, and Ascertia shall have no obligation to assess or monitor the Customer's compliance with such laws; and

(ii) bears sole responsibility for assessing whether the Products and any related Support and Advisory Services are suitable for the intended Processing of Customer Data in accordance with applicable Data Protection Laws.

2.2 Confidentiality

Ascertia shall treat all Customer Personal Data as Confidential Information of the Customer in accordance with the Agreement and shall ensure that any personnel authorised to Process such Personal Data are subject to appropriate written or statutory confidentiality obligations.

3. Security

3.1 Technical and Organisational Measures

Ascertia has implemented, and shall continue to maintain, appropriate technical and organisational measures intended to safeguard the confidentiality, integrity, availability, and resilience of Customer Data and to protect against Security Incidents. The Customer remains responsible for properly configuring the Products and for making use of the security features and functionality provided by Ascertia, taking into account the nature of the Customer Data processed. A description of Ascertia's current technical and organisational measures is available in Schedule 3. The Customer acknowledges that such measures may evolve in line with technological developments, and that Ascertia may amend or update them from time to time, provided that any such changes do not result in a material reduction in the overall level of security applicable to the Cloud Products during the applicable Subscription Term.

3.2 Security Incidents

Ascertia shall notify the Customer without undue delay and, where practicable, within seventy-two (72) hours of becoming aware of a Security Incident. Ascertia shall use reasonable endeavours to investigate the Security Incident, limit its impact, and address the underlying cause to the extent such matters are within Ascertia's reasonable control. Taking into account the nature of the Processing and the information reasonably available to it, Ascertia shall, upon request, provide the Customer with information reasonably required to enable the Customer to comply with its Security Incident notification obligations under applicable Data Protection Laws. Any notification provided by Ascertia pursuant to this Section does not constitute an admission of fault or liability.

4. Sub-processing

4.1 General Authorisation

By entering into this DPA, the Customer grants Ascertia a general authorisation to engage Sub-processors to Process Customer Personal Data in connection with the provision of the Products and any associated Support and Advisory Services. Ascertia shall ensure that each Sub-processor is appointed under a written agreement, or equivalent, that imposes data protection obligations on the Sub-processor which are no less protective than those set out in this DPA and are consistent with Applicable Data Protection Laws. Ascertia shall remain responsible to the Customer for the performance of its Sub-processors' data protection obligations in relation to the Processing of Customer Personal Data under the Agreement.

4.2 Approved Sub-processors

Ascertia's authorised Sub-processors are listed in Schedule 4 of this DPA. The Customer acknowledges and agrees that Ascertia may engage the Sub-processors identified in Schedule 4 to Process Customer Personal Data in accordance with the terms of this DPA.

4.3 Customer Acceptance and Termination Right

Where the Customer does not agree to the engagement of one or more Sub-processors listed in Schedule 4, or any future updates to that list, the Customer's sole and exclusive remedy shall be to cease use of the Products and terminate the Agreement (or the relevant Order) in accordance with the termination provisions of the Agreement. Continued use of the Products constitutes the Customer's acceptance of Ascertia's use of the Sub-processors listed in Schedule 4.

5. Assistance and Cooperation

5.1 Data Subject Rights

Having regard to the nature of the Processing, Ascertia shall provide the Customer with reasonable and timely assistance to support the Customer in responding to requests from data subjects to exercise their rights in relation to Customer Personal Data, including rights of access, rectification, erasure, restriction of processing, objection, and data portability.

5.2 Regulatory and Compliance Cooperation

Taking into account the nature of the Processing and upon the Customer's reasonable request, Ascertia shall provide reasonable assistance to enable the Customer to comply with its obligations under applicable Data Protection Laws, including in connection with data protection impact assessments and consultations with supervisory authorities, to the extent that the Customer is unable to fulfil such obligations independently using available Documentation.

5.3 Third Party Requests

To the extent permitted by Law, Ascertia shall promptly inform the Customer of any valid and binding legal or governmental request requiring disclosure of Customer Personal Data. Where Ascertia receives a request, inquiry, or communication from any other third party (including a supervisory authority or a data subject) relating to the Processing of Customer Personal Data, Ascertia shall refer such request to the Customer and shall not disclose any information unless disclosure is legally required.

6. Deletion and Return of Customer Personal Data

6.1 During the Subscription Term

Throughout the Subscription Term, the Customer and its authorised Users may, using the functionality of the Cloud Products, access, retrieve, and delete Customer Personal Data.

6.2 After Expiry or Termination

Upon the expiry or termination of the Agreement, Ascertia shall delete all Customer Personal Data in accordance with the applicable Documentation. Notwithstanding the foregoing, Ascertia may retain Customer Personal Data where: (i) retention is required under applicable Data Protection Laws; or (ii) such data is retained in line with Ascertia's standard backup or record retention practices. In each case, Ascertia shall continue to ensure the confidentiality of any retained Customer Personal Data, comply with the relevant provisions of this DPA, and refrain from any further Processing of such data except as strictly required by applicable Data Protection Laws.

7. Audit Rights

7.1 Audit Information and Reports

Ascertia undergoes regular audits conducted by independent third-party auditors and/or internal audit functions. Subject to the Customer entering into an appropriate non-disclosure agreement with Ascertia, Ascertia shall, upon request, provide the Customer with a summary of relevant audit reports to enable the Customer to assess Ascertia's compliance with the applicable audit standards and the requirements of this DPA. Where the Customer is unable, acting reasonably, to confirm such compliance based on the information provided, Ascertia shall, on a confidential basis, respond in writing to reasonable information requests relating to its Processing of Customer Personal Data, provided that this right may be exercised no more than once in any twelve (12) month period.

7.2 On-Site Audits and Inspections

Only where the Customer cannot reasonably verify Ascertia's compliance with this DPA through the measures described in Section 7.1 above, or where an audit is required by applicable Data Protection Laws or a competent supervisory authority, the Customer or its duly authorised representatives may, at the Customer's cost, conduct an audit or inspection during the term of the Agreement to assess such compliance. Any audit shall:

(a) take place during Ascertia's normal business hours and be subject to at least sixty (60) days' prior written notice, unless a shorter notice period is mandated by applicable Data Protection Laws or a regulatory authority;

(b) be subject to reasonable confidentiality obligations requiring the Customer and its authorised representatives to treat as confidential any information disclosed that is confidential by its nature;

(c) be carried out no more than once in any twelve (12) month period; and

(d) be limited in scope to information directly relevant to the Customer.

8. International and Region-Specific Provisions

Where Ascertia Processes Personal Data that is subject to Applicable Data Protection Laws in any of the regions identified in Schedule 2 (Region-Specific Terms), the provisions applicable to the relevant region(s) shall apply in addition to this DPA, including any terms governing international transfers of Personal Data, whether such transfers occur directly or through onward transfers.

9. Definitions

"Applicable Data Protection Law" means any Law that applies to the Processing of Personal Data under the Agreement.

"Controller" means any natural or legal person, public authority, agency, or other body that, either alone or jointly with others, determines the purposes and means of Processing Personal Data.

"Customer Personal Data" means any Personal Data contained within Customer Data and/or Customer Materials that Ascertia Processes exclusively on behalf of the Customer pursuant to the Agreement. For the avoidance of doubt, this includes Personal Data contained in any files, materials, or attachments submitted by the Customer or its Users as part of technical support requests.

"Cloud Products" means Ascertia's hosted, cloud-based software products and platforms made available to the Customer under the Agreement, including SigningHub, together with any associated functionality, features, updates, and related Support and Advisory Services.

"Personal Data" means any information relating to an identified or identifiable individual, or that otherwise qualifies as "personal data", "personal information", "personally identifiable information", or equivalent terms under Applicable Data Protection Law.

"Processing", and the terms **"Process"** and **"Processed"**, refer to any operation or series of operations performed on Personal Data or sets of Personal Data, whether carried out by automated means or otherwise, including collection, recording, organisation, structuring, storage, adaptation or modification, retrieval, consultation, use, disclosure by transmission, dissemination or other means of making available, alignment or combination, restriction, erasure, or destruction.

"Processor" means any entity that Processes Personal Data on behalf of a Controller.

"Security Incident" means any breach of security resulting in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Customer Data Processed by Ascertia and/or its Sub-processors. For the purposes of this definition, references to "Processing" include the Processing of both Personal Data and Customer Data.

"Sub-processor" means any third party, including Ascertia Affiliates, engaged by Ascertia to Process Customer Personal Data.

SCHEDULE 1 DESCRIPTION OF PROCESSING

1. **Categories of Data Subjects**

The Personal Data Processed relates to the Customer and the Customer's Users.

2. **Categories of Personal Data**

The categories of Personal Data Processed consist of Customer Personal Data, the specific content and nature of which are determined and controlled exclusively by the Customer and its Users.

3. **Special Categories of Data**

The Customer or its Users may submit content to the Cloud Products that includes: (i) data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; (ii) genetic data, biometric data used for the purpose of uniquely identifying an individual, data concerning health, or data relating to an individual's sex life or sexual orientation; or (iii) data relating to criminal convictions and offences (together, "Sensitive Data"**).** Any such Sensitive Data is determined and controlled solely by the Customer and its Users.

4. **Frequency of Processing and Transfer**

The Processing and any associated transfer of Personal Data occurs on a continuous basis.

5. **Nature of the Processing**

Ascertia Processes Personal Data for the purpose of delivering the Products and any associated Support and Advisory Services in accordance with the Agreement, including this DPA. Further details regarding the nature of the Processing, including any data transfers, are set out in the applicable Orders for the relevant Products and in the Documentation describing the technical features and functionality of the Products. Such Processing may include, without limitation, the automated collection, organisation, storage, transmission, and other forms of making Personal Data available.

6. **Purposes of processing**

6.1 Customer Data

Acting as a Processor and in accordance with the Customer's Documented Instructions, Ascertia Processes Customer Data for the following purposes:

(a) to deliver, operate, and enhance the Products and any associated Support and Advisory Services for the Customer, and to enable the use of the Products' features and functionality in accordance with the Documentation and instructions provided by Users through the Cloud Products, including for the investigation of Security Incidents and the identification and resolution of issues, defects, and errors;

(b) to administer and enforce the applicable terms of use; and

(c) to comply with Ascertia's applicable legal obligations.

6.2 Processing as Controller

Ascertia acts as a Controller in respect of certain Personal Data as described in Ascertia's Privacy Policy. Nothing in this DPA restricts or prevents Ascertia from Processing Personal Data in that capacity.

7. **Duration of the Processing**

Ascertia will Process Customer Personal Data for the duration of the Agreement, subject to the deletion and return obligations set out in Section 6 (Deletion and Return of Customer Personal Data) of this DPA.

8. **Transfers to Sub-processors**

Ascertia may disclose or transfer Customer Personal Data to Sub-processors in accordance with, and to the extent permitted by, Section 4 (Sub-processing) of this DPA.

SCHEDULE 2 REGION-SPECIFIC TERMS

Unless expressly defined in this DPA or in the Agreement, any capitalised terms used in this Schedule shall have the meanings assigned to them in Section 5 of this Schedule. References to Tables and Annexes in this Schedule are references to the corresponding tables and annexes of the EU SCCs and IDTAs and UK Addendum, as applicable.

1. Europe, United Kingdom and Switzerland

1.1 Customer Instructions

In addition to the requirements set out in Section 2.1 (Customer Instructions) and Schedule 1 (Description of Processing) of this DPA, Ascertia shall Process Customer Personal Data only in accordance with the Customer's Documented Instructions, including in relation to any transfers of such Customer Personal Data to a third country or an international organisation, unless Processing is required by Applicable Data Protection Law to which Ascertia is subject. In such circumstances, Ascertia shall notify the Customer of the relevant legal requirement prior to Processing, unless the applicable law prohibits such notification on important grounds of public interest. Ascertia shall also promptly notify the Customer if it becomes aware that any of the Customer's Processing instructions are inconsistent with Applicable Data Protection Law.

1.2 Transfers from Europe

Where Personal Data subject to EU Data Protection Law is transferred, whether directly or by onward transfer, to a recipient located in a country outside Europe that is not covered by an adequacy decision, the following shall apply:

The EU Standard Contractual Clauses are incorporated into this DPA by reference on the following basis:

(a) For the purposes of the EU SCCs:

(i) the Customer acts as the data exporter, and Ascertia acts as the data importer;
(ii) Module Two (Controller to Processor) applies where the Customer acts as a Controller of Customer Personal Data and Ascertia Processes such data as a Processor;
(iii) Module Three (Processor to Processor) applies where the Customer acts as a Processor of Customer Personal Data and Ascertia Processes such data as an additional Processor; and
(iv) by entering into this DPA, each Party is deemed to have executed the EU SCCs as of the effective date of the Agreement.

(b) In relation to each applicable Module of the EU SCCs:

(i) the optional docking clause in Clause 7 is excluded;
(ii) Clause 9, Option 2 applies, and the advance notice period for changes to Sub-processors is as set out in Section 4 (Sub-processing) of this DPA;
(iii) the optional wording in Clause 11 does not apply;
(iv) Clause 17, Option 1 applies, and the EU SCCs are governed by the laws of Italy;
(v) pursuant to Clause 18(b), any disputes shall be submitted to the courts of Italy; and
(vi) the Appendix to the EU SCCs shall be completed as follows:

- the information required for Annex I(A) is set out in the Agreement and/or the applicable Orders;
- the information required for Annex I(B) is contained in Schedule 1 (Description of Processing) of this DPA; and
- the competent supervisory authority for Annex I(C) shall be determined in accordance with Applicable Data Protection Law.
- The information required for Annex II is available in Schedule 3 of this DPA.

1.3 Swiss Transfers

Where Personal Data subject to Swiss Data Protection Law is transferred, whether directly or through onward transfer, to a recipient in a country that is not subject to an adequacy decision, the EU Standard Contractual Clauses shall apply in accordance with Section 1.2 (European Transfers) above, subject to the following adaptations:

(a) All references in the EU SCCs to "Regulation (EU) 2016/679" will be interpreted as references to Swiss Data Protection Law, and references to specific Articles of "Regulation (EU) 2016/679" will be replaced with the equivalent article or section of Swiss Data Protection Law; all references to the EU Data Protection Law in this DPA will be interpreted as references to Swiss Data Protection Law.

(b) In Clause 13, the competent supervisory authority is the Swiss Federal Data Protection and Information Commissioner.
(c) In Clause 17, the EU SCCs are governed by the laws of Switzerland.

(d) In Clause 18(b), disputes will be resolved before the courts of Switzerland.

(e) All references to Member State will be interpreted to include Switzerland and Data Subjects in Switzerland are not excluded from enforcing their rights in their place of habitual residence in accordance with Clause 18(c) of the EU SCCs.

1.4 United Kingdom Transfers

Where Personal Data subject to UK Data Protection Law is transferred, whether directly or by onward transfer, to a recipient located outside the United Kingdom in a country that is not subject to an adequacy decision, the following shall apply:

The EU Standard Contractual Clauses shall apply in accordance with Section 1.2 (European Transfers) above, subject to the following modifications:

(a) By entering into this DPA, each Party is deemed to have executed the UK Addendum or, where applicable, the UK International Data Transfer Agreement (UK IDTA).

(b) For the purposes of Table 1 of the UK Addendum, the Parties' primary contact details are set out in the Agreement and/or the applicable Orders.

(c) For Table 2 of the UK Addendum, the information relating to the applicable version of the EU SCCs, the selected Modules, and the relevant clause elections to which the IDTA is attached is specified in Section 1.2 (European Transfers) of this Schedule.

(d) For Table 3 of the UK Addendum:

(i) The information required for Annex 1A is located in the Agreement and/or relevant Orders.

(ii) The Information required for Annex 1B is located in Schedule 1 (Description of Processing) of this DPA.

(iii) The information required for Annex II is located in Schedule 3 (Technical and Organisational measures) of this DPA.

(iv) The information required for Annex III is located in Section 4 (Sub-processing) of this DPA.

(e) In Table 4 of the UK Addendum, both the data importer and data exporter may end the UK Addendum.

2. US Transfers

The following terms apply where Ascertia Processes Personal Data subject to the US State Privacy Laws:

2.1. To the extent that Customer Personal Data includes personal information regulated under US State Privacy Laws and is Processed by Ascertia on behalf of the Customer in its capacity as a Service Provider or Processor, Ascertia shall Process such Customer Personal Data in compliance with the applicable requirements of the US State Privacy Laws. This includes providing a level of privacy protection consistent with the standards required under those laws and Processing such data solely in accordance with the Customer's Documented Instructions, as necessary to carry out the limited and specified purposes set out in Section 6.1 of Schedule 1 (Description of Processing). Ascertia shall not:

(a) retain, use, disclose, or otherwise Process such Customer Personal Data for any commercial purpose other than the limited and expressly defined purposes set out in this DPA, the Agreement, and/or any applicable Order, except as otherwise permitted under applicable US State Privacy Laws;

(b) "sell" or "share" such Customer Personal Data, as those terms are defined under US State Privacy Laws; or

(c) retain, use, disclose, or otherwise Process such Customer Personal Data outside of the scope of the direct business relationship with the Customer, or combine such Customer Personal Data with personal information obtained from other sources, except where such activities are expressly permitted under applicable US State Privacy Laws.

2.2. Ascertia shall notify the Customer if it determines that it is no longer able to comply with its obligations under applicable US State Privacy Laws.

2.3 The Customer may take reasonable and appropriate measures to prevent, stop, or remediate any unauthorised Processing of Customer Personal Data.

2.4 To the extent that the Customer discloses or otherwise makes Deidentified Data available to Ascertia, or where Ascertia generates Deidentified Data from Customer Personal Data, in each case acting in its capacity as a Service Provider, Ascertia shall:

(a) implement reasonable safeguards designed to ensure that such Deidentified Data cannot reasonably be used to identify, relate to, or be linked with a specific individual or household;

(b) make a public commitment to maintain and Process the Deidentified Data solely in de-identified form and to refrain from any attempts to re-identify such data, except to the limited extent necessary to assess and validate the effectiveness of its de-identification measures in accordance with applicable US State Privacy Laws; and

(c) prior to disclosing or making Deidentified Data available to any third party, including Sub-processors, contractors, or other recipients (each, a **"**Recipient**"**), ensure that such Recipient is contractually bound to comply with the requirements of this Section 2.4, including the obligation to impose equivalent restrictions on any onward recipients.

3. South Korea Transfers

3.1 The Customer represents and warrants that it has provided all required notices and obtained any consents, authorisations, or other rights necessary under applicable South Korean privacy laws to permit Ascertia to Process Personal Data in accordance with the Agreement.

3.2 To the extent that the Customer discloses or otherwise makes Deidentified Data available to Ascertia, Ascertia shall:

(a) ensure that such Deidentified Data is maintained and Processed only in de-identified form and refrain from attempting to re-identify the data; and

(b) prior to disclosing Deidentified Data to any third party, including Sub-processors, contractors, or other recipients (each, a **"**Recipient**"**), require such Recipient by contract to comply with the obligations set out in this Section 3.2, including the obligation to impose equivalent requirements on any onward recipients.

4. Vietnam Transfers

4.1 The Customer represents and warrants that it has provided all required notices and obtained any consents, authorisations, or other lawful bases required under applicable Vietnamese data protection laws to permit Ascertia to Process Personal Data in accordance with the Agreement and this DPA.

4.2 To the extent that the Customer discloses or otherwise makes Deidentified Data available to Ascertia, Ascertia shall:

(a) ensure that such Deidentified Data is maintained and Processed solely in de-identified form and shall not attempt to re-identify such data, except where permitted by applicable Vietnamese data protection laws; and

(b) prior to disclosing Deidentified Data to any third party, including Sub-processors, contractors, or other recipients (each, a "Recipient"), ensure that such Recipient is contractually bound to comply with obligations equivalent to those set out in this Section 4.2, including the obligation to impose equivalent requirements on any onward recipients.

5. Definitions

"Deidentified Data" means data that cannot reasonably be used to identify, relate to, or otherwise be associated with an individual data subject.

"Vietnamese Data Protection Law" means Decree No. 13/2023/ND-CP on the Protection of Personal Data, together with any implementing regulations, guidance, amendments, or replacements in force from time to time.

"Data Privacy Framework" refers to the EU–U.S. Data Privacy Framework, the UK Extension to the EU–U.S. Data Privacy Framework, and the Swiss–U.S. Data Privacy Framework self-certification programme administered by the United States Department of Commerce.

"Europe" means, for the purposes of this DPA, the Member States of the European Union together with the states comprising the European Economic Area.

"EU Data Protection Law" includes: (i) Regulation (EU) 2016/679 of the European Parliament and of the Council concerning the protection of natural persons with respect to the Processing of Personal Data and the free movement of such data (the General Data Protection Regulation or GDPR); and (ii) the EU e-Privacy Directive (Directive 2002/58/EC), in each case as amended, superseded, or replaced from time to time.

"EU SCCs" means the standard contractual clauses adopted by the European Commission pursuant to Implementing Decision (EU) 2021/914 of 4 June 2021 for the transfer of Personal Data to third countries under Regulation (EU) 2016/679, as amended, superseded, or replaced from time to time.

"Service Provider" has the meaning assigned to that term under the California Consumer Privacy Act.

“South Korea Privacy Law” means the Personal Information Protection Act of the Republic of Korea, together with its implementing decrees and regulations, as amended, superseded, or replaced from time to time.

“Swiss Data Protection Law” means the Swiss Federal Act on Data Protection and its implementing regulations, as amended, superseded, or replaced from time to time.

“UK Addendum” means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner, version B1.0, effective from 21 March 2022, as amended, superseded, or replaced from time to time.

“UK International Data Transfer Agreement” or **“**UK IDTA**”** means the International Data Transfer Agreement issued by the UK Information Commissioner under section 119A of the Data Protection Act 2018 for transfers of Personal Data to third countries, as amended, superseded, or replaced from time to time.

“UK Data Protection Law” means the Data Protection Act 2018 together with the GDPR as incorporated into United Kingdom law pursuant to section 3 of the European Union (Withdrawal) Act 2018, in each case as amended, superseded, or replaced from time to time.

“US State Privacy Laws” means all applicable state-level laws in force in the United States governing the protection and Processing of Personal Data, including, without limitation, the California Consumer Privacy Act as amended by the California Privacy Rights Act, together with any implementing regulations (CCPA).

SCHEDULE 3 – TECHNICAL AND ORGANISATIONAL MEASURES

1. Technical Measures

1.1 Cryptographic Security & Public Key Infrastructure (PKI)

Ascertia employs industry-standard, PKI-based cryptographic mechanisms to protect personal data and electronic transactions. SigningHub supports Advanced Electronic Signatures (AES) and Qualified Electronic Signatures (QES) in accordance with the eIDAS Regulation. Cryptographic controls are implemented using strong, publicly recognised algorithms and key lengths appropriate to the security requirements and regulatory expectations.

SigningHub supports long-term validation (LTV) of signed documents through the use of trusted timestamps, certificate status information (e.g. OCSP/CRL), and evidence records, ensuring the integrity and evidential value of documents remains verifiable over time, even after certificate expiry or revocation.

For Qualified Electronic Signatures (QES) and other regulated signature use cases, SigningHub integrates with Qualified Trust Service Providers (QTSPs) using the Cloud Signature Consortium (CSC) API. In such cases, private signature keys are held and managed by the relevant QTSP within a Secure Signature Creation Device (SSCD) or Qualified Signature Creation Device (QSCD) environment, which may utilise a SAM appliance operated either by Ascertia technology or by a third-party provider, depending on the QTSP's infrastructure.

1.2 Key Management and Cryptographic Protection

For certain use cases, including electronic seals (eSeals) and specific user key protection scenarios, cryptographic keys are generated, stored, and managed using Microsoft Azure Key Vault. Azure Key Vault provides hardware-backed key protection and secure key lifecycle management controls, including restricted access, role-based permissions, and audit logging.

Cryptographic operations involving protected keys are performed within secure cryptographic boundaries, ensuring that private keys are not exposed in plaintext form. Access to key material is strictly controlled and limited in accordance with the principle of least privilege.

1.3 Secure Architecture & Trust Service Integration

Ascertia's signing infrastructure is designed following secure-by-design and defence-in-depth principles.

Where SigningHub is used in conjunction with Qualified Trust Service Providers (QTSPs) for eIDAS-compliant Qualified Electronic Signatures, the trust service environment, including any Secure Signature Creation Device (SSCD) or Qualified Signature Creation Device (QSCD), is operated and certified by the relevant QTSP. Such environments may include SAM appliances implemented either using Ascertia technology or third-party technology, depending on the QTSP's deployment model.

Ascertia's role in such integrations is limited to securely interfacing with the QTSP via standardised APIs (including the CSC API), ensuring secure transmission of signature requests and associated data, without direct custody or control of the end user's qualified private keys.

1.4 Data Protection in Transit and at Rest

SigningHub protects data transmitted over public and private networks using industry-standard secure communication protocols (such as TLS), ensuring confidentiality and integrity during data transmission.

Where applicable, data stored within the SigningHub environment is protected using encryption and other security controls appropriate to the sensitivity of the data and the deployment model. These measures reduce the risk of unauthorised disclosure or alteration of personal data.

1.5 Access Control & Authentication

Access to SigningHub systems and administrative functions is restricted based on the principle of least privilege. Logical access controls ensure that users can only access data and functionality necessary for their role.

SigningHub supports strong authentication mechanisms, including two-factor authentication (2FA), to reduce the risk of unauthorised access. Administrative access is further restricted and monitored to prevent misuse or privilege escalation.

1.6 Monitoring, Logging & Audit

SigningHub implements comprehensive logging and audit capabilities to record security-relevant events, including authentication attempts, administrative actions, and signing activities. Logs are protected against unauthorised modification and are retained in accordance with applicable regulatory and contractual requirements.

These measures support incident detection, forensic analysis, and compliance with legal and regulatory obligations.

1.7 Availability, Resilience & Backup

SigningHub is designed to support high availability and operational resilience. Depending on the deployment model, measures may include redundancy, failover mechanisms, and regular data backups.

Backup and recovery procedures are implemented to ensure the availability and integrity of data in the event of system failure, human error, or security incidents.

1.8 Secure Development & Vulnerability Management

Ascertia follows secure software development practices throughout the product lifecycle, including design, development, testing, and maintenance. Security vulnerabilities are assessed and remediated in a timely manner based on risk.

Regular updates and patches are provided to address security issues and maintain the security posture of the SigningHub platform.

2. Organisational Measures

2.1 Information Security Governance

Ascertia maintains information security policies and procedures aligned with recognised security and compliance frameworks. These policies govern access control, cryptographic key management, incident management, and data protection obligations.

2.2 Personnel Security & Confidentiality

Personnel with access to systems processing personal data are subject to appropriate confidentiality obligations. Access is granted based on role and business need, and revoked promptly when no longer required.

2.3 Incident Management & Breach Response

Ascertia maintains procedures to detect, respond to, and manage security incidents, including personal data breaches. Incidents are assessed promptly, and appropriate corrective and preventive actions are taken in line with contractual and legal obligations.

2.4 Sub-processors & Third Parties

Where sub-processors are engaged, Ascertia applies due diligence and contractual safeguards to ensure an appropriate level of data protection and security consistent with this Schedule and applicable data protection laws.

SCHEDULE 4 – LIST OF SUB-PROCESSORS

Sub-Processor	Applicable Products	Nature and Purpose of Processing	Categories of Personal Data	Location of Processing	Privacy and Security Information
Microsoft Azure	SigningHub	Cloud hosting and infrastructure services, including storage and processing of Customer Data	Customer Personal Data, as determined and controlled by the Customer, including data uploaded or generated through the SigningHub service	Global data centres (region dependent on customer configuration)	https://learn.microsoft.com/en-us/compliance/regulatory/gdpr
Stripe	SigningHub	Payment processing and subscription management	Customer account and billing contact data	United States and other global locations	https://stripe.com/privacy
MaxMind	SigningHub	IP geolocation and fraud detection	IP addresses and related technical metadata	United States	https://www.maxmind.com/en/privacy-policy
SendGrid (Twilio)	SigningHub	Transactional and service-related email delivery	Contact details and message metadata necessary to deliver communications	United States and other global locations	https://www.twilio.com/legal/data-protection-addendum
Twilio	SigningHub	SMS and telecommunications services	Contact details (e.g. phone numbers) and message metadata	United States and other global locations	https://www.twilio.com/legal/data-protection-addendum
Clickatell	SigningHub	SMS delivery and messaging services	Contact details (e.g. phone numbers) and message metadata	Ireland and United States	https://www.clickatell.com/legal/privacy-policy/
Google Crashlytics	SigningHub	Application performance monitoring and crash reporting	Technical data, including device and application diagnostics	United States and other Google infrastructure locations	https://firebase.google.com/support/privacy
Google Firebase	SigningHub	Push notification services	Device identifiers and notification delivery data	United States and other Google infrastructure locations	https://firebase.google.com/support/privacy
Microsoft OneDrive	SigningHub	Cloud storage integrations for document handling	Customer Personal Data contained in documents uploaded by Users	Global data centres	https://privacy.microsoft.com/
Google Drive	SigningHub	Cloud storage integrations for document handling	Customer Personal Data contained in documents uploaded by Users	Global data centres	https://workspace.google.com/terms/dpa_terms.html
Dropbox	SigningHub	File storage and document synchronisation	Customer Personal Data contained in stored files	United States and other Dropbox data centres	https://www.dropbox.com/en/privacy
Taxamo (Vertex)	SigningHub	Tax calculation and VAT determination	Billing and transaction-related data	United States	https://www.taxamo.com/privacy-policy/
Site24x7	SigningHub	System monitoring and uptime management	Technical and operational metadata	European Union, United States, and India	https://www.site24x7.com/privacy.html
Microsoft Azure Key Vault	SigningHub	Secure storage and management of cryptographic keys, certificates and secrets used to protect Customer Data and system authentication	Encryption keys and security credentials associated with Customer Data (does not independently process Customer Personal Data in content form)	Global data centres (region dependent on customer configuration)	https://learn.microsoft.com/en-us/compliance/regulatory/gdpr
Worldpay	SigningHub	Payment processing and transaction handling for subscription and related services	Customer billing information, payment card data (processed in accordance with PCI-DSS requirements), billing contact details	United Kingdom, European Economic Area and other global locations as required for payment processing	https://privacy.worldpay.com/policies