Verisq AI Data Processing Addendum v1.1

Version 1.1
Last Updated: November 16, 2025

This Data Processing Addendum ("**DPA**") supplements the agreement between Customer and Verisq Inc. ("**Verisq AI**") into which it is incorporated by reference (the "**Agreement**").

---

1. Definitions

Unless otherwise defined below, all capitalized terms in this DPA shall have the meaning given to them in the Agreement.

- **Adequate Country**
  A country that the European Commission, the United Kingdom's Information Commissioner's Office, or the Swiss Federal Data Protection and Information Commissioner (as applicable based on respective area of competence) has determined as ensuring an adequate level of data protection.
- **Applicable Data Protection Law**
  All applicable data protection and privacy laws and regulations relating to the processing of personal data under the Agreement, including, where applicable: EU Data Protection Law, UK Data Protection Law, Swiss Data Protection Law, and US Data Protection Law.
- **Authorized Affiliate**
  A Customer Affiliate which is an Authorized User under the Agreement and is subject to Applicable Data Protection Law of a jurisdiction requiring the signature of a binding contract between the controller and the processor.
- **Controller**, **data subject**, **personal data**, **processor**, and **special categories of personal data**
  Have the meanings given in Applicable Data Protection Law. Any references in this DPA to "personal data", "processor", and "controller" shall be deemed to include their equivalent concepts under the CCPA and CPRA, respectively, "personal information", "service provider", and "business".
- **Cloud Services**
  The Verisq AI hosted software-as-a-service solutions identified in an Order Form or

Purchase Schedule, including associated dashboards, APIs, and modules, but excluding Professional Services.

- **Data**
  Personal data processed by Verisq AI on behalf of Customer in connection with the Agreement, as more particularly described in Appendix 2.

- **Data Protection Claim**
  Any claim, action, demand, or proceeding arising out of or relating to (a) Verisq AI's processing of personal data on behalf of Customer, including any Privacy Breach; or (b) alleged violation of Applicable Data Protection Law by Verisq AI in connection with the Cloud Services.

- **Data Privacy Framework**
  The EU–US Data Privacy Framework, the UK Extension to the EU–US Data Privacy Framework, and the Swiss–US Data Privacy Framework, set forth by the U.S. Department of Commerce and the European Commission, the UK Government, and the Swiss Federal Administration.

- **EDPB Recommendations**
  The European Data Protection Board's Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.

- **EEA**
  The European Economic Area.

- **EU Data Protection Law**
  (a) The EU General Data Protection Regulation (2016/679) (GDPR);
  (b) The EU Directive 2002/58/EC (e-Privacy Directive); and
  (c) Any EU Member State laws made under or pursuant to any of the foregoing;
  in each case as amended or superseded from time to time.

- **Processing** and **Process**
  Any operation or set of operations performed upon the Data by automated means or otherwise, including the sale or sharing, combination, retention, use, or disclosure of Data.

- **Professional Services**
  Configuration, implementation, consulting, training, or other professional services performed by Verisq AI as described in a Statement of Work or similar document, but excluding the provision of Cloud Services.

- **Privacy Breach**
  Has the meaning given in Section 7 (a Privacy Breach is any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to the Data).
- **Swiss Data Protection Law**
  The Swiss Federal Act on Data Protection (Revised FADP) of 2020, as amended or superseded from time to time.
- **Third Country**
  A country outside of the EEA, the UK, or Switzerland (as applicable) which is not an Adequate Country.
- **UK Data Protection Law**
  The data privacy legislation adopted by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019/419 as supplemented by the Data Protection Act 2018 and the UK GDPR (Retained Regulation (EU) 2016/679), as amended or superseded from time to time.
- **US Data Protection Law**
  (a) The California Consumer Privacy Act of 2018 (CCPA), as amended and integrated by the California Privacy Rights Act of 2020 (CPRA); and
  (b) Any similar or equivalent state privacy laws in the United States to the extent applicable to the processing of Data.

---

2. Instructions & Scope of Processing

2.1 Appointment and Permitted Purpose

Subject to the Agreement and this DPA, Customer appoints Verisq AI as its processor (or service provider, as applicable) to process the Data for the purposes of providing the Services to Customer and complying with Verisq AI's obligations under the Agreement as further described in Appendix 2 (or as reasonably instructed in writing by Customer, to the extent consistent with—and not in addition to—the terms of the Agreement) (the "**Permitted Purpose**"). Customer shall ensure that its instructions comply with Applicable Data Protection Law and that the Data submitted to Verisq AI is limited to what is necessary in relation to the purposes for which it is processed.

2.2 Limitations on Processing

Verisq AI shall not Process the Data outside the direct business relationship between the Parties and for any purpose (including any commercial purpose) other than the Permitted Purpose, or as otherwise permitted by Applicable Data Protection Law.

2.3 Conflicting or Unlawful Instructions

Verisq AI shall promptly notify Customer if it determines that (a) a Customer instruction infringes Applicable Data Protection Law, or (b) it can no longer meet its obligations under Applicable Data Protection Law.

2.4 Compliance

Each Party shall comply with its respective obligations under Applicable Data Protection Law.

2.5 Service Provider / Processor Role; No Sale or Sharing

Verisq AI shall Process the Data solely as a "processor" or "service provider" (as those terms are defined under Applicable Data Protection Law) on behalf of Customer and only for the Permitted Purpose. Verisq AI certifies that it shall not:

- sell or share the Data, including for cross-context behavioral advertising;
- retain, use, or disclose the Data for any purpose other than the Permitted Purpose or as otherwise permitted by Applicable Data Protection Law and this DPA; or
- combine the Data with personal information that Verisq AI receives from other sources, except as necessary to provide, secure, and improve the Services in accordance with Customer's documented instructions.

---

3. International Transfers & Data Localization

3.1 Transfers to Third Countries

If any Data is protected under EU Data Protection Law, then Verisq AI shall only transfer such Data to a Third Country subject to measures to ensure the transfer is compliant with EU Data Protection Law. Such measures may include transferring the Data to a recipient that has:

- achieved binding corporate rules authorization in accordance with EU Data Protection Law; or
- executed standard contractual clauses adopted or approved by the European Commission.

Data shall be stored in the geographic regions specified in Appendix 3, Section 2.

3.2 Supplementary Measures

Prior to transferring Data to a Third Country, Verisq AI shall review the adequacy of data protection in the Third Country and shall apply, where necessary, the appropriate measures to ensure that the transferred Data is subject to an essentially equivalent protection as that guaranteed in its original jurisdiction. The supplementary measures implemented by Verisq AI pursuant to the EDPB Recommendations may be further described in Verisq AI's documentation or Support Portal.

Verisq AI shall:

- notify Customer if Verisq AI is unable to comply with its legal or contractual obligations related to international transfers under EU Data Protection Law; and
- suspend the applicable transfers of Data until it is able to comply with such obligations.

---

4. Security & Confidentiality

4.1 Technical and Organizational Measures

Taking into account the state of the art, the costs of implementation, and the nature, scope, context, and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Verisq AI shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk (in accordance with Applicable Data Protection Law) to protect the Data from:

- accidental or unlawful destruction; and
- loss, alteration, unauthorized disclosure of, or access to the Data (a "**Privacy Breach**"),

including encryption standards as detailed in Appendix 3, Section 3 (AES-256 encryption for data at rest and TLS 1.2 or higher for data in transit).

4.2 Certifications and Security Program

Verisq AI maintains an information security management program aligned with recognized industry frameworks (including, for example, NIST CSF and CIS Controls) and designed to protect the confidentiality, integrity, and availability of the Services and Customer Data.

Verisq AI may, in its sole discretion and without prior approval from Customer, perform or engage third parties to perform security assessments, vulnerability scanning, penetration testing, and other security testing of its own networks, infrastructure, and the Services. Verisq AI will use commercially reasonable efforts to conduct such testing in a manner that does not materially and adversely disrupt Customer's use of the Services. Any summaries or results of such testing that Verisq AI elects to share with Customer shall constitute Verisq AI Confidential Information.

All penetration or other security testing initiated by Customer on or against the Services (including any Verisq AI–hosted environment) must be conducted only in a designated testing environment and pursuant to a separate written agreement between the Parties that defines scope, timing, and coordination requirements.

Verisq AI is working towards SOC 2 Type 2 and may, once available, provide related information or summaries to Customer upon request, subject to reasonable confidentiality and use restrictions.

4.3 Confidentiality and Access Controls

Verisq AI shall treat the Data as Confidential Information under the Agreement and shall only share it with authorized persons who need access to the Data for the Permitted Purpose and are subject to a statutory or contractual duty of confidentiality.

Access to Data shall be controlled according to the framework specified in Appendix 3, Section 4, which includes:

- restricting access to personnel and subcontractors with a legitimate need to know;
- applying role-based access control, authentication, logging, and least-privilege principles; and
- monitoring access consistent with Verisq AI's security program.

Verisq AI does not represent or warrant that access by its personnel will be technically impossible in all circumstances, but will maintain controls designed to minimize and monitor such access.

---

5. Subprocessing

5.1 Approved Subprocessors

The list of Verisq AI's subprocessors ("**Subprocessors List**") is as follows and may be updated from time to time:

- Microsoft Azure
- Amazon Web Services (AWS)

Customer consents to Verisq AI engaging subprocessors to process the Data for the Permitted Purpose. Verisq AI shall:

- enter into a written contract with each subprocessor requiring the subprocessor to protect the Data in accordance with Applicable Data Protection Law, including privacy obligations no less protective of Data than this DPA; and
- be responsible for any breach of this DPA caused by its subprocessors.

5.2 Changes to Subprocessors

Verisq AI shall update the Subprocessors List at least thirty (30) days in advance of any change to the list, except to the extent shorter notice is required due to an emergency.

5.3 Customer Objections

Customer may object to Verisq AI's appointment of a subprocessor within thirty (30) days following Verisq AI's notification of a change in the Subprocessors List, provided such objection is based on reasonable data protection grounds. Following such an objection, Verisq AI will, if possible, either:

- reasonably assist Customer to configure the Services to disable the use of the objected-to subprocessor; or
- use commercially reasonable efforts to replace the subprocessor.

---

6. Consultation, Assistance & Data Subject Requests

6.1 DPIAs and Consultations

Taking into account the nature of the processing, and to the extent required by Applicable Data Protection Law, Verisq AI shall provide Customer with reasonable cooperation and such information available to Verisq AI (that is not available to Customer) to enable Customer to:

- conduct a data protection impact assessment or transfer impact assessment related to Customer's use of the Services; and
- consult competent supervisory authorities prior to a processing operation under the Agreement.

6.2 Data Subject Requests (Support Role Only)

Taking into account the nature of the processing and the functionality of the Services, Verisq AI shall assist Customer, by appropriate technical and organizational measures, in ensuring that Customer can access and export Data required to respond to requests from data subjects to exercise their rights under Applicable Data Protection Law (including rights of access, correction, deletion, restriction, portability, and objection).

Customer is solely responsible for:

- determining how to respond to such requests; and
- communicating with data subjects and regulators regarding such requests and any responses.

If Verisq AI receives a request directly from a data subject relating to the Data, Verisq AI shall promptly notify Customer and shall not respond to such request except on the documented instructions of Customer or as required by Applicable Data Protection Law.

6.3 Audit and Information Rights

Upon Customer's written request, and no more than once in any twelve (12) month period (except following a proven Privacy Breach), Verisq AI shall make available to Customer information reasonably necessary to demonstrate compliance with this DPA and Applicable Data Protection Law, which may include:

- summaries of third-party audit reports (such as SOC 2 Type 2 reports); and
- certificates for its ISO Certifications.

To the extent such documentation is not reasonably sufficient, Customer may, at its own cost and subject to reasonable advance notice and confidentiality obligations, conduct (or appoint a third party to conduct) a security and privacy audit of Verisq AI's relevant facilities, systems, and records, during regular business hours and in a manner that does not unreasonably interfere with Verisq AI's operations.

---

7. Privacy Breaches

If Verisq AI becomes aware of a Privacy Breach, Verisq AI shall:

- inform Customer **without undue delay**; and

- provide reasonable information and cooperation to Customer so that Customer can fulfill any data breach reporting obligations it may have under Applicable Data Protection Law.

Verisq AI shall further take such reasonably necessary measures and actions to mitigate the effects of the Privacy Breach and shall keep Customer informed of all material developments in connection with the Privacy Breach.

---

8. Deletion or Return of Data

Following termination of the Agreement, Customer shall have sixty (60) days to export its Data from the Cloud Services. After such time has passed, Verisq AI may destroy all Data in its possession or control.

This requirement shall not apply to the extent that:

- Verisq AI is required by Applicable Law to retain some or all Data; or
- Data is archived on Verisq AI's back-up and support systems, which shall be deleted in accordance with its security procedures,

provided that Verisq AI shall continue to protect such Data in accordance with its obligations herein.

---

9. Authorized Affiliates & Liability

9.1 Application to Authorized Affiliates

To the extent required by Applicable Data Protection Law, Customer enters into this DPA on behalf of itself and on behalf of its Authorized Affiliates who are controllers of Data processed by Verisq AI. Except where expressly indicated otherwise, and only where applicable, for the purposes of this DPA only, "Customer" shall include Customer and Authorized Affiliates.

9.2 Enforcement

All rights of Authorized Affiliates under this DPA shall be exercised by Customer on behalf of the Authorized Affiliate and only Customer (and not Authorized Affiliates) shall be permitted to directly enforce this DPA (including on behalf of an Authorized Affiliate), except where Applicable Data Protection Law requires an Authorized Affiliate to enforce directly.

9.3 Aggregate Liability

For the avoidance of doubt, each Party's and its Affiliates' aggregate liability to the other Party and its Affiliates, arising out of or relating to the Agreement (including this DPA and any addendum between Verisq AI and an Authorized Affiliate) shall be calculated on a total aggregate basis in accordance with the liability provisions of the Agreement. For purposes of the liability provisions in the Agreement, Authorized Affiliates' losses shall be considered Customer's losses.

---

10. Survival

The obligations set out in the sections of this DPA addressing:

- Security & Confidentiality,
- Subprocessing,
- Privacy Breaches,
- Deletion or Return of Data,
- Authorized Affiliates & Liability,

and any other provisions of this DPA that by their nature are intended to survive, shall survive termination or expiry of the Agreement for so long as Verisq AI retains any Data.

Appendix 1: Verisq AI Information Security Controls

Verisq AI has organized and implemented technical and organizational measures for personal data protection according to NIST CSF, CIS Controls, and the STAR Cloud Controls Matrix (CCM) self-assessment to support its information security and data protection program. The measures include the following types of controls (non-exhaustive summary):

- **Information Security Policies** – Management direction and support for information security in accordance with business requirements and relevant laws and regulations.
- **Organization of Information Security** – Framework for initiating and controlling information security implementation and operations.
- **Enterprise Risk Management** – Methodology for the assessment and treatment of risks associated with the loss of confidentiality, integrity, and availability of information, and definition of acceptable risk levels.
- **Access Control** – Principles governing information access based on business and security requirements.
- **Operations Security** – Procedures for the proper management of IT systems, including change management, capacity management, malware protection, and logging/monitoring.
- **Communications Security** – Securing networks and communications, including network segregation and protection of information in networks.
- **System Acquisition, Development, and Maintenance** – Security requirements for procurement, development, and maintenance of information systems.
- **Supplier Relationships** – Vendor risk management, including due diligence, contractual security requirements, and monitoring of third-party suppliers.
- **Incident Management** – Responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents.
- **Business Continuity Management** – Processes to ensure availability of information and continuity of critical services.

Verisq AI may update or supplement these measures over time, provided such updates do not materially reduce the overall level of protection for Data.

Appendix 2: Details of Processing

Categories of Data Subjects

Personal data may relate to:

- Customer's employees, contractors, agents, consultants;
- Customer's vendors and business partners;
- Data subjects whose personal data is processed by Customer and managed within the Cloud Services; and
- Data subjects submitting or implicated in data subject rights requests handled by the Services.

Categories of Personal Data

Personal data processed by Verisq AI typically includes:

- Identifying data such as name, username, email address, phone number, job title, employer information;
- Technical identifiers such as IP address, device identifiers, cookies or similar identifiers;
- Data subject request metadata (request type, timestamps, fulfillment details, workflow routing);
- Business contact data for vendors and partners (names, business emails, phone numbers, work addresses, roles);
- Any personal data submitted to the Services or to Verisq AI or its Affiliates in the course of performing the Services, as configured by Customer.

Special Categories of Data

Customer may, at its sole discretion, submit special categories of personal data to the Services, including information about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health, sex life or sexual orientation, medical and criminal records, genetic data, or biometric data for the purposes of uniquely identifying a natural person.

Restricted Data Types (PCI, PHI, Certain SPI)

Notwithstanding the foregoing, Customer shall not submit to the Services any of the following ("**Restricted Data**") unless the Parties have first executed a written addendum or agreement specifying additional safeguards and any additional fees applicable to such processing:

- PCI-DSS-protected payment card data (including but not limited to magnetic stripe or chip data, CAV2/CVC2/CVV2/CID numbers, and PINs);
- Protected Health Information ("PHI") as defined in HIPAA or similar health information laws;
- Certain categories of Sensitive Personal Information ("SPI") that create heightened regulatory obligations, including without limitation:
    - full financial account numbers,
    - government-issued identification numbers (such as Social Security numbers, national IDs, driver's license numbers),
    - precise geolocation data,
    - biometric identifiers, and
    - information regarding minors where such information is regulated as SPI or special category data.

Customer is solely responsible for ensuring it has a lawful basis and all necessary notices and consents to submit any personal data, including special categories of personal data or SPI, to the Services.

Purpose and Nature of Processing

Personal data is primarily processed for the following purposes:

- Providing the Cloud Services and Professional Services under the Agreement;
- Supporting configuration, implementation, integration, and customer success activities;
- Providing helpdesk and support services;
- Monitoring, maintaining, and improving the security and performance of the Services;
- Supporting Customer's internal privacy and security workflows, including third-party risk management and data subject rights management; and

- Fulfilling Customer's documented instructions related to privacy compliance use cases.

Processing operations may include:

- Collection of personal data entered by users into the Cloud Services;
- Storage, structuring, and organization of personal data within tenant environments;
- Use of personal data to route, track, and audit data subject rights requests;
- Use of personal data for access control and authentication;
- Aggregation and reporting (in de-identified or pseudonymized form) for performance and security analytics.

Duration of Processing

The Data may be processed for the duration of the Agreement and for such additional period during which the Data is retained in accordance with this DPA and the Agreement (for example, during the post-termination export and back-up retention periods).

Appendix 3: Data Collection and Access Controls

1. Data Collection by Module

1.1 Data Subject Rights Management (DSAR) Module

- **Required Data Elements**:
  Name, email address, phone number.
- **Optional Data Elements**:
  Physical address, date of birth, account identifiers, internal customer or employee IDs.
- **Purpose**:
  Solely for privacy request processing, identity matching, workflow routing, and audit trail.
- **Retention**:
  Data related to data subject rights requests is retained for as long as reasonably necessary to:
  - process the request,
  - maintain an audit trail of request handling, and
  - comply with applicable legal and contractual obligations,
    and is thereafter deleted or anonymized in accordance with Verisq AI's data retention policies.

1.2 Azure AD SSO Platform Access Module

- **Data Elements**:
  Azure login ID, name, email address, optionally phone number and group/role identifiers.
- **Purpose**:
  Secure platform access management, Single Sign-On, and authentication event logging.
- **Retention**:
  As required for access management, security monitoring, and audit logging in accordance with Verisq AI's retention policies.

1.3 Third Party Risk Management (TPRM) Module

- **Data Elements**:
  Vendor/third-party information (generally business contact information), including company names, business email addresses, phone numbers, mailing addresses, and roles/titles of vendor contacts.
- **Purpose**:
  Third-party risk assessment and management, including vendor onboarding, due diligence, and ongoing risk monitoring.
- **Retention**:
  As specified in the Agreement and applicable Order Forms or as required to maintain vendor risk records and audit trails.

1.4 Other Verisq AI Modules

- **Data Elements**:
  As configured by Customer for the relevant module, limited to the data types necessary to support the module's functionality.
- **Purpose**:
  To provide the module-specific functionality selected by Customer in accordance with the Agreement (for example, consent management, records of processing activities, data mapping, mailbox scanning, and related governance workflows).
- **Retention**:
  As specified in the Agreement and applicable Order Forms, or as otherwise disclosed in Verisq AI's data retention policies, consistent with the intended use of each module.

---

2. Data Storage and Regionalization

2.1 Geographic Storage

- **US Tenants**:
  All Data is stored in cloud infrastructure regions located in the United States, provisioned via Microsoft Azure and/or Amazon Web Services (AWS).
- **EU Tenants**:
  All Data is stored in cloud infrastructure regions located within the European Union, provisioned via Microsoft Azure and/or Amazon Web Services (AWS), in compliance with GDPR regionalization requirements.

- **Data Isolation**:
  Each tenant's Data is logically isolated from other tenants' Data.

2.2 Subprocessor Locations

All subprocessors listed in Section 5.1 of this DPA shall Process Data only in regions consistent with the geographic storage requirements defined above, unless otherwise agreed in writing or required by Applicable Data Protection Law.

---

3. Encryption Standards

3.1 Encryption at Rest

All sensitive Data is encrypted at rest using AES-256 (or an equivalent industry-standard algorithm).

3.2 Encryption in Transit

All Data transmissions are protected using TLS 1.2 or higher.

3.3 End-to-End Encryption for Outbound Communications

Where the Services send Data to data subjects or external recipients as part of DSAR or similar workflows, Verisq AI uses encryption to protect such Data in transit. Such Data may be encrypted at source and may remain unreadable within Verisq AI's systems depending on the specific workflow configuration and Customer's choices.

---

4. Access Control Framework

4.1 Tenant User Access

Tenant users (Customer's authorized users) have access to:

- their own tenant's Data in cleartext form, subject to Customer's internal role-based permissions;
- all Data attributes collected for their organization as configured by Customer; and
- controls to manage access permissions within their tenant.

4.2 Verisq AI Personnel and Subcontractor Access

- **Need-to-Know Access**:
  Verisq AI personnel and any subcontractors or consultants engaged by Verisq AI

may access Data only to the extent reasonably necessary to operate, support, secure, or improve the Services, or as otherwise required to comply with Applicable Data Protection Law or binding legal process.

- **Confidentiality**:
  All such individuals are bound by appropriate statutory or contractual confidentiality obligations.
- **Technical and Organizational Controls**:
  Verisq AI applies role-based access control, authentication, logging, and least-privilege principles designed to minimize and monitor access to sensitive Data.
- **No Absolute Access Waiver**:
  Verisq AI does not represent or warrant that access by its personnel will be technically impossible in all circumstances, but will maintain controls consistent with the Security & Confidentiality section of this DPA and its information security program.