ETHICS SUITE

Ethics Suite Data Processing Addendum

Updated 12/29/25

This Data Processing Agreement ("DPA") forms part of the agreement between Ethics Suite and clients (**"Client"** or **"Controller"**) who use our services, and it governs how we process personal data on behalf of our customers in accordance with applicable data protection laws, including the General Data Protection Regulation (GDPR), the UK GDPR, the Data Protection Acts 1998-2019 of Ireland and the revised Swiss Federal Act on Data Protection (revFADP). By entering into a service agreement with us, such as a Subscriber Agreement, Terms of Service, Consulting Agreement, or End User Licensing Agreement (individually and collectively, **"Agreement"**), you agree to the terms of this DPA.

If you have any questions about this DPA or how we handle your data, please contact us at privacy@ethicssuite.com. As defined below, the parties hereby agree that the terms and conditions set out below shall govern Ethics Suite's Processing of Client Personal Data in carrying out the objectives and responsibilities set forth in the Agreement (the "**Services**"). This DPA does not extend to the Processing of information, including the Processing of Personal Data, that is outside of the scope of the Services or the Agreement, or to the Client or Client Personal Data if neither is subject to Data Protection Laws. Except as modified herein, the terms of the Agreement shall remain in full force and effect. By agreeing to the Agreement, Client hereby agrees to the terms of this DPA.

1. **Definitions**. For purposes of this DPA, the following terms shall have the meanings set forth below. Capitalized terms used but not otherwise defined in this DPA will have the meaning given to them in the Agreement.

1.1. "**Affiliate**" means an entity that owns or controls, is owned or controlled by, or is under common control or ownership with, either Client or Ethics Suite respectively. "Control," for purposes of this definition, means the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise.

1.2. "**Client Personal Data**" means only the Personal Data of a Client described in **Exhibit 1** which is Processed by Ethics Suite, or by a Subprocessor, on behalf of Client.

1.3. "**Data Protection Laws**" means, to the extent that they apply to the Client, the EU's General Data Protection Regulation, the Data Protection Acts 1998-2019 of Ireland, the UK Data Protection Act, 2018, and any U.S. comprehensive state privacy law, such as the California Consumer Privacy Act, Colorado Privacy Act, or similar laws, as amended, replaced, or superseded from time to time.

1.4. "**Data Subject**" means the identified or identifiable person to whom Personal Data relates.

1.5. "**Personal Data**" means any information relating to an identified or identifiable natural person, as defined under applicable Data Protection Laws (including 'personal information' as defined under U.S. state privacy laws).

1.6. "**Security Incident**" means any confirmed accidental, unauthorized, or unlawful disclosure of, personal data breach, or access to, Client Personal Data Processed by Ethics Suite or any Subprocessor.

1.7. "**Process**" means any operation or set of operations that is performed upon Personal Data, whether or not by automatic means, such as access, collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, return or destruction and "Processing" shall be construed accordingly.

1.8. "**Subprocessor**" means a subcontractor engaged by Ethics Suite or its affiliates to Process Client Personal Data as part of the performance of the Services.

Subject to Section 1.1, references herein to terms which are defined in the EU GDPR, UK GDPR or FADP shall have the same meanings herein.

2. **Compliance with International Data Protection Laws.** Where Processor has its main establishment within the European Union, including a registered office in Ireland at Ethics Suite Europe Ltd, 3rd Floor, Percy Exchange, 8–34 Percy Place, Dublin D04 P5K3, Ireland, no separate representative under Article 27 GDPR is required for processing activities subject to the EU GDPR. Where Processor processes Personal Data subject to the UK GDPR without an establishment in the United Kingdom, Processor shall designate a representative in the United Kingdom in accordance with Article 27 of the UK GDPR. The name and contact details of such representative shall be made available to Controller and Data Subjects upon request.

   Processor shall comply with all applicable data protection and privacy laws, regulations, and regulatory guidance, including, where applicable, the EU General Data Protection Regulation (Regulation (EU) 2016/679) ("EU GDPR"), the Data Protection Acts 1998-2018 of Ireland, the UK General Data Protection Regulation, the Data Protection Act 2018, and UK Data Use and Access Act 2025 (DUAA) ("UK Data Protection Laws"), and the Swiss Federal Act on Data Protection ("FADP"), in connection with its Processing of Client Personal Data under this Agreement. Processor shall implement and maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk and shall provide Controller with such cooperation as is reasonably necessary to enable Controller to meet its own obligations under applicable Data Protection Laws.

3. **Compliance with California Consumer Privacy Act (CCPA/CPRA):** Where the Controller is subject to the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020:
   - **3.1. Service Provider Role:** Ethics Suite shall act as a "service provider" (as defined under CCPA/CPRA) and shall not:
     - 3.1.1. Sell or share personal information;
     - 3.1.2. Retain, use, or disclose personal information for any purpose other than to provide the Services or as permitted by the Agreement;
     - 3.1.3. Retain, use, or disclose personal information outside of the direct business relationship with the Client.
   - **3.2. Consumer Requests:** Ethics Suite shall provide reasonable assistance to the Client in responding to verifiable consumer requests to exercise their rights under the CCPA/CPRA, including rights of access, deletion, correction, and limitation of sensitive personal information.
   - **3.3. Certifications:** Ethics Suite certifies that it understands and will comply with the restrictions set forth in this Section.

4. **Records of Processing Activities (ROPA).** Processor shall maintain a record of all categories of Processing activities carried out on behalf of Controller in accordance with Article 30(2) GDPR and make such records available to Controller or any Supervisory Authority upon request.

5. **Data Protection Impact Assessment (DPIA) Cooperation.** Processor shall provide Controller with reasonable cooperation and assistance to enable Controller to conduct data protection impact assessments and consult with Supervisory Authorities, as required under Articles 35 and 36 GDPR.

6. **Assistance to Controller.** Processor shall, taking into account the nature of the Processing and the information available to it, provide reasonable assistance to Controller to enable Controller to: (a) respond to requests from Data Subjects exercising their rights under applicable Data Protection Laws; (b) comply with Controller's obligations relating to the security of Processing under Article 32 GDPR; and (c) meet any obligations to notify Personal Data Breaches to Supervisory Authorities or Data Subjects under Articles 33 and 34 GDPR. .

   Such assistance shall be provided only to the extent that Controller cannot reasonably fulfil its obligations without Processor's cooperation and the Controller shall discharge any reasonable, documented costs incurred by Processor in providing such assistance.

7. **Controller Responsibilities.**
   - **7.1. Lawful Basis and Instructions.** The Controller shall ensure that it has established all necessary lawful bases and provided all required notices to Data Subjects under Applicable

Data Protection Laws before directing the Processor to process any Personal Data. The Controller shall be solely responsible for the accuracy, quality, and legality of Personal Data and the means by which it acquires such data.

7.2. Data Subject Rights. The Controller shall be responsible for responding to requests from Data Subjects under Applicable Data Protection Laws, including but not limited to requests for access, rectification, erasure, restriction, portability, and objection. The Processor shall provide reasonable assistance to the Controller in fulfilling such requests in accordance with Section **Assistance to Controller**.

7.3. Retention and Deletion. The Controller shall determine the applicable retention periods for Personal Data and provide instructions to the Processor regarding the return or deletion of Personal Data at the end of the processing relationship, in accordance with Section 13 (**Deletion or Return of Client Personal Data)**.

7.4. Transparency and Communications. The Controller shall be responsible for providing clear and sufficient information to Data Subjects about the processing of their Personal Data, including disclosures relating to the use of the Processor and any international transfers.

7.5. Security and Internal Controls. The Controller shall maintain appropriate technical and organizational measures to ensure compliance with Applicable Data Protection Laws, including ensuring that Personal Data is collected and transmitted to the Processor in a secure manner.

7.6. Provision of External Reporting Information. The Controller is solely responsible for informing Data Subjects, including potential whistleblowers, of their rights under applicable law and of the availability of external reporting channels (including competent regulatory or governmental authorities) as required under the EU Whistleblower Protection Directive (EU) 2019/1937 and related national implementing laws. Processor shall not provide such information directly to reporters unless explicitly instructed in writing by the Controller.

8. Processing of Client Personal Data.

8.1. Details of the Processing of Client Personal Data pursuant to the Agreement are set forth in **Exhibit 1** attached to this DPA.

8.2. Ethics Suite will only Process Client Personal Data for the purposes of providing the Services specified in the Agreement and only in accordance with Customer's documented instructions, which may be specific instructions or standing instructions of general application in relation to the performance of Ethics Suite's obligations under this DPA, unless otherwise required under applicable Data Protection Laws to which Ethics Suite is subject, in which case Ethics Suite shall notify Customer prior to such Processing unless prohibited by law.

8.2.1. Ethics Suite understands, and will comply with, the obligations and restrictions imposed on it by applicable Data Protection Laws in its role as a service provider and/or Processor;

8.2.2. Client instructs Ethics Suite to Process Personal Data to perform the Services and as described in this DPA and the Agreement. Ethics Suite shall notify Client immediately if Ethics Suite determines that it can no longer meet its obligations under applicable Data Protection Laws or if, in Ethics Suite's opinion, Client's instructions infringe applicable Data Protection Laws;

8.2.3. Ethics Suite shall take reasonable steps to ensure that access to Client Personal Data is limited to those employees, agents, Affiliates, and Subprocessors who have a need to know or otherwise access Client Personal Data to enable Ethics Suite to perform its obligations or responsibilities under this DPA and the Agreement, and who are bound in writing to protect the confidentiality of the Client Personal Data (the restrictions set forth in this section shall not restrict Ethics Suite's ability to Process Client Personal Data where required to do so by applicable laws to which Ethics Suite is subject; provided, however, Ethics Suite shall promptly notify Client of such legal requirement before Processing, unless such law prohibits such notification);

8.2.4. Ethics Suite shall Process Client Personal Data under the Agreement in compliance with applicable Data Protection Laws, including providing the same level of privacy protection required by applicable Data Protection Laws. Ethics Suite will notify Client if Ethics Suite determines it or its Subprocessor(s) cannot meet its obligations under applicable Data Protection Laws, in which case Client may, upon thirty (30) days' notice, take reasonable and appropriate steps to stop and remediate unauthorized Processing of Personal Data.

8.2.5. Notwithstanding any other provision in this Section 8, Ethics Suite may internally use deidentified Client Personal Data relating solely to individuals located in the United States for the limited purpose of improving the quality or security of the Services, provided such use complies with applicable U.S. privacy laws and does not involve reidentification.

8.3. Ethics Suite shall not:

8.3.1. retain, use, or disclose Client Personal Data for any purpose other than for the limited and specified purpose of performing its responsibilities under the Agreement;

8.3.2. share, sell, rent, release, assign, transfer, disclose, disseminate, make available, transfer, or otherwise communicate orally, in writing, or by electronic or other means Client Personal Data to another person or entity for: (a) monetary or other valuable consideration; or (b) cross-context behavioral advertising for the benefit of a business in which no money is exchanged;

8.3.3. aggregate, anonymize, or otherwise deidentify Personal Data without the prior written authorization of Client except as needed to perform the Services. To the extent that it deidentifies Client Personal Data, Ethics Suite will (i) take reasonable measures to ensure that the information cannot be associated with an individual; (ii) publicly commit to maintain and use the information in deidentified form and not to attempt to reidentify it; (iii) implement technical safeguards that prohibit reidentification; (iv) implement business processes that specifically prohibit reidentification; (v) implement business processes that prevent inadvertent release of deidentified information; (vi) make no attempt to reidentify the information; and (vii) contractually obligate any recipients of the deidentified information to comply with all provisions in this paragraph; or

8.3.4. combine Client Personal Data with Personal Data Ethics Suite receives from or on behalf of another person or entity or collects from its own interactions with a Data Subject except to perform a business purpose as defined in regulations adopted pursuant applicable Data Protection Laws.

9. **Security**. Ethics Suite represents, warrants and undertakes that it shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including, as appropriate, the measures referred to in Article 32 of the GDPR, and shall ensure that all such safeguards comply with applicable Data Protection Laws. Such safeguards are further specified in **Exhibit 2** attached to this DPA. In assessing the appropriate level of security, Ethics Suite shall take into account the risks that are presented by Processing, including without limitation the risks of a Security Incident.

10. **Security Incident**. In the event of a Security Incident impacting Client Personal Data, Ethics Suite shall notify Client without undue delay after becoming aware of a Security Incident and shall cooperate with Client and take commercially reasonable steps to assist in the investigation, mitigation, and remediation of a Security Incident.

11. **Subprocessors**.

11.1. Client authorizes Ethics Suite and each Ethics Suite Affiliate to appoint (and permit each Subprocessor appointed in accordance with this Section 11 to appoint) Subprocessors in accordance with this Section 11 and any restrictions in the Agreement and applicable Data Protection Laws, including the Standard Contractual Clauses and UK Addendum, if applicable.

11.2. Ethics Suite and each Ethics Suite Affiliate may continue to use those Subprocessors already engaged by Ethics Suite or any Ethics Suite Affiliate as of the date of this DPA, including those listed in **Exhibit 1**. Ethics Suite shall give Client prior written notice of the appointment of any new Subprocessor, including full details of the Processing to be undertaken by the Subprocessor, and Client must inform Ethics Suite of any objection to such new Subprocessor within seven (7) days of such notice or such Subprocessor shall be deemed fully accepted by Client.

11.3. With respect to any Subprocessor, Ethics Suite shall enter into a written agreement with each Subprocessor obligating the Subprocessor to comply with terms that are at least as restrictive as those imposed on Ethics Suite under this DPA. Ethics Suite shall remain fully liable to Client for the acts or omissions of its Subprocessors.

12. Data Subject Rights.

12.1. Ethics Suite will provide such assistance, including taking any appropriate technical and organizational measures, as Client requests to help Client fulfill its obligations under applicable Data Protection Laws to respond to Data Subject requests.

12.2. Notwithstanding its obligations under this Section, Ethics Suite is not obligated to respond to a Data Subject request directly from a Data Subject and does not otherwise assume any liability or responsibility for responding to Data Subject requests.

13. Deletion or Return of Client Personal Data. Ethics Suite shall promptly destroy all copies of Client Personal Data in its possession, or in the possession of its Subprocessor (a) upon Client's request; or (b) within ninety (90) calendar days of the effective date of termination. Notwithstanding the requirements in this paragraph, Ethics Suite may retain Client Personal Data if required by applicable Data Protection Laws, but only to the extent and for such period as required by such legal requirement. Ethics Suite shall notify Client in writing if it believes that such a legal requirement exists. If required by law to retain Client Personal Data, Ethics Suite shall store the Client Personal Data solely on encrypted backup or archive locations, continue to safeguard such data in accordance with this DPA, and only Process such Client Personal Data as necessary for the purpose specified in the applicable Data Protection Laws requiring such storage.

14. Compliance and Audits.

14.1. Upon Client's request, Ethics Suite shall provide such assistance as Client reasonably requires to ensure compliance with Client's obligations under applicable Data Protection Laws, including, but not limited to, any data protection impact assessments and/or consultations with government authorities pursuant to applicable Data Protection Laws.

14.2. Ethics Suite shall make available to Client all information necessary to demonstrate Ethics Suite's compliance with this DPA, as well as any applicable Data Protection Laws, and shall allow for and contribute to audits, including inspections, by Client, or a third-party auditor mandated by Client, in order to assess Ethics Suite's compliance (collectively, "**Audits**").

14.3. Client may perform such Audits not more than once per year or more frequently if required by applicable Data Protection Laws. Audits must be conducted off premises during regular business hours, subject to Ethics Suite policies, and may not unreasonably interfere with Ethics Suite business activities.

14.4. Client must provide Ethics Suite with any Audit reports or findings generated in connection with any Audit at no charge, unless prohibited by law. Client may use the Audit reports only for the purposes of meeting its Audit requirements under applicable Data Protection Laws and/or monitoring and confirming compliance with the requirements of this DPA. The Audit reports shall constitute confidential information of the parties.

14.5. Nothing in this Section 14 shall require Ethics Suite to breach any duties of confidentiality owed to any of its customers or employees.

14.6. Under the following circumstances, Client agrees to accept those findings in lieu of requesting an Audit of the controls covered by the report: (a) the requested Audit scope is addressed in a similar Audit report performed by a qualified third-party auditor for Ethics Suite within twelve (12) months of Client's request; (b) if permitted by applicable Data Protection Laws; and (c) Ethics Suite confirms there are no known material changes in the controls audited. All Audits are at Client's sole cost and expense. Any request for Audit assistance requiring the use of resources different from or in addition to those required for provision of the Services will be considered an additional Service for which reasonable additional fees may be charged. Ethics Suite reserves the right to require Client's written agreement to pay for such fees before providing such Audit assistance.

14.7. Information and Audit rights of the Client only arise under this Section 14 to the extent that the Agreement does not otherwise give the Client information and Audit rights meeting the relevant requirements of applicable Data Protection Law.

15. International Data Transfers

15.1. Ethics Suite will not transfer Client Personal Data outside its jurisdiction of establishment necessary to perform the Services and subject to an applicable transfer mechanism under Data Protection Laws. Insofar as the Agreement involves the transfer of Client Personal Data from a jurisdiction where applicable Data Protection Laws requires that additional steps, or safeguards, be imposed before the data can be transferred to a second jurisdiction, Ethics Suite agrees to cooperate with Client to take appropriate steps to comply with applicable Data Protection.

15.2. If the Processing (including storage) of Client Personal Data involves the transfer of Client Personal Data from the European Economic Area ("**EEA**") to a jurisdiction outside of the EEA where the transfer would be prohibited by applicable Data Protection Laws in the absence of standard contractual clauses or another adequate transfer mechanism as approved by the European Commission, the parties agree that such transfer(s) will be carried out in accordance with and subject to the standard contractual clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council annexed to the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 ("**EU SCCs**") as set out in **Exhibit 3** attached to this DPA. To the extent there is any conflict between this DPA and the EU SCCs, the terms of the EU SCCs will prevail.

15.3. Ethics Suite processes United Kingdon ("**UK**") Personal Data within the European Union or other jurisdictions deemed adequate under UK law. No transfer to a third country without adequacy will occur unless instructed by the Controller, in which case the mechanism in Section 15.2 applies. If the Processing (including storage) of Client Personal Data involves the transfer of Client Personal Data from the UK to a jurisdiction outside of the UK where the transfer would be prohibited by applicable Data Protection Laws in the absence of standard contractual clauses or another adequate transfer mechanism as approved by the UK Information Commissioners Office ("**ICO**"), the parties agree that such transfer(s) will be carried out in accordance with and subject to the International Data Transfer Agreement A1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022 ("**UK IDTA**") as set out in **Exhibit 4** attached to this DPA. To the extent there is any conflict between this DPA and the UK IDTA, the terms of the UK IDTA will prevail.

15.4. If the Processing (including storage) of Client Personal Data involves the transfer of Client Personal Data from Switzerland to a jurisdiction outside of Switzerland where the transfer would be prohibited by applicable Data Protection Laws in the absence of standard contractual clauses or another adequate transfer mechanism as approved by the Swiss Federal Data Protection and Information Commissioner ("**FDPIC**"), the parties agree that such transfer(s) will be carried out in accordance with and subject to the EU SCCs as amended by the Addendum to the EU SCCs attached hereto as **Exhibit 5**.

15.5. Insofar as the Agreement involves the transfer of Client Personal Data from any other jurisdiction where applicable Data Protection Laws requires that additional steps, or safeguards, be imposed before the data can be transferred to a second jurisdiction, Ethics Suite agrees to cooperate with Client to take appropriate steps to comply with applicable Data Protection Laws.

16. Location Selection & Routing of Reports

16.1. Processor provides technical functionality within the Ethics Suite platform that allows Clients to self-select the ultimate location of data storage and hosting in the United States or European Union. As described above, the Parties agree to carry out any external transfers in accordance with the applicable SCC in **Exhibits 3, 4 or 5**.

16.2. Processor does not verify the accuracy of Client's selection. The Controller remains solely responsible for:

16.2.1. Determining the applicability of data protection laws (including GDPR and other regional requirements) to any given report;

16.2.2. Establishing and maintaining a lawful basis for processing;

16.2.3. Ensuring compliance with applicable cross-border data transfer rules; and

16.2.4. Responding to Data Subject rights requests and fulfilling all obligations under Articles 12–22 of the GDPR.

16.2.5. Processor's role is limited to facilitating the routing of reports in accordance with Controller's instructions.

17. Cross-Border Access. The Parties acknowledge that certain U.S.-based personnel of Ethics Suite and Client may require remote access to Personal Data stored in the EU. Such access shall be limited to the following two distinct categories. For purposes of this Section, "access" includes any viewing, retrieval, or other remote processing of Client Personal Data from outside the EEA/UK/Switzerland.

17.1. Operational Access: Granted to designated administrative users in the ordinary course of providing the Services, for the purposes of case management, report review, and other agreed business functions. Such users may require full access to Personal Data to perform case management, report review, and other agreed business functions.

17.2. Maintenance Access: Granted to IT or support personnel solely for the purpose of system administration, troubleshooting, or maintenance, and only where access to Personal Data is strictly necessary. All cross-border access shall be subject to Standard Contractual Clauses, as described in Section 15 and attached in Exhibit 3 (EU), Exhibit 4 (UK), and Exhibit 5 (Switzerland), as applicable, Transfer Impact Assessments, role-based access controls, encryption in transit and at rest, and detailed logging. Maintenance Access shall be temporary, supervised where feasible, and subject to masking or pseudonymization unless full access is technically required to resolve the issue. Processor shall review and update its Transfer Impact Assessments at least annually or upon material changes to the transfer circumstances.

18. Liability. The parties each represent and warrant to each other that they have read and understand the requirements of all applicable Data Protection Laws and will be responsible for their own compliance with them.

18.1. Ethics Suite shall not have any liability to Client to the extent the basis of liability arises from failure by Client to obtain any necessary consents to collect, use, transfer, or otherwise Process Client Personal Data, or failure by Client to fully comply with the Agreement, this DPA, or applicable Data Protection Laws.

18.2. Client represents and warrants that, if required, it has provided notice that the Client Personal Data is being Processed consistent with applicable Data Protection Laws.

18.3. Each party agrees to indemnify, defend, and hold harmless the other party from and against any claims, demands, losses, liabilities, fines, penalties, costs, and expenses arising out of or relating to its own acts and omissions that do not comply with applicable Data Protection Laws. This duty to indemnify, defend, and hold harmless includes fines that may be imposed by a governing authority and any and all reasonable attorneys' fees and court costs.

18.4. Each party's liability under or in connection with this DPA is subject to the limitations on liability contained in the Agreement, to the extent permitted by law.

19. **General Terms**. This DPA supersedes any prior data processing agreements, addenda, or similar terms between the parties. Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA will remain valid and in force. The invalid or unenforceable provision shall be either: (a) amended as necessary to ensure its validity and enforceability, while preserving the intent of the provision as closely as possible or, if this is not possible; (b) construed in a manner as if the invalid or unenforceable part had never been contained therein. In the event of any conflict between the Agreement and this DPA, this DPA will govern. If any variation is required to this DPA as a result of a change in applicable Data Protection Laws, the parties agree to discuss and negotiate in good faith any necessary variation to this DPA. The obligations contained in this DPA, including the Exhibits, shall not restrict Ethics Suite in its rights and/or obligations to: (i) comply with federal, state, or local laws, or to comply with a court order or subpoena to provide information or legal holds; or (ii) to comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities.

List of Exhibits:

Exhibit 1: Details of Processing

Exhibit 2: Description of Technical and Organizational Security Measures

Exhibit 3: EU SCCs

Exhibit 4: UK IDTA

Exhibit 5: Addendum to the EU SCCs for Transfers out of Switzerland

Exhibit 1

Details of Processing

1. Subject Matter of Processing

The subject-matter of Processing of Client Personal Data by Ethics Suite is the performance of the Services pursuant to the Agreement.

2. Nature and Purpose of Processing

Client Personal Data will be processed by Ethics Suite solely as necessary to provide the Services under the Agreement and strictly in accordance with the Client's documented instructions. Such processing will be limited to the following activities:

1. Receiving data – The receipt of Client Personal Data into the Services' systems, including the secure collection, electronic transmission, and automated logging of:
2. Whistleblower reports and associated case data submitted by authorized users or Data Subjects.
3. User account registration and access control information for authorized users of the platform.
4. Holding data – The secure storage, hosting, organization, and structuring of Client Personal Data in the case management platform and associated systems.
5. Protecting data – Implementing technical and organizational measures to protect Client Personal Data, including encryption, access controls, authentication management, audit logging, and security testing.
6. Updating data (limited) – Making changes to user account and access control information (e.g., usernames, roles, passwords, contact details) and, only upon Client's documented instruction, making changes to case data.
7. Sharing data (limited) – Making Client Personal Data available:
    a. To Client's authorized users via the Services; and
    b. To approved Subprocessors (e.g., cloud hosting providers) solely for the purposes of providing the Services.
8. Erasing data – The deletion or destruction of Client Personal Data from the Services upon Client's instruction, in accordance with retention periods or termination provisions in the Agreement.

3. Duration of Processing

Subject to Section 7 of the DPA, Ethics Suite will Process Client Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing.

4. Categories of Data Subjects

The Personal Data Processed may concern the following categories of Data Subjects:

- Client employees (including full-time, part-time, and temporary staff)
- Client contractors and contingent workers
- Client officers, directors, and board members
- Third parties referenced in hotline reports (e.g., customers, suppliers, vendors, business

partners, or other individuals whose Personal Data is included in a report)

- Authorized users of the case management platform (e.g., designated investigators, HR personnel, compliance officers)

5. Types of Personal Data

The Processing may involve the following types of Personal Data, as determined by the Client and submitted via the Services:

- Identifying information: names, job titles, contact details (e.g., email address, phone number, physical address).
- Employment-related information: department, work location, manager or supervisor details, employment status, role, or other HR records.
- Account and authentication information: usernames, system roles, credentials, and audit logs relating to authorized users of the Services.
- Report content: narrative descriptions, allegations, witness statements, supporting evidence, and any other Personal Data included by the reporter or the Client in a hotline report or case file.
- Third-party information: Personal Data of individuals referenced in a report, such as customers, suppliers, vendors, or other business contacts.
- Technical and metadata: IP addresses, browser or device identifiers, access logs, and other telemetry generated by the use of the Services.

Sensitive or special categories of Personal Data (as defined in Article 9 UK GDPR/EU GDPR), and Personal Data relating to criminal convictions and offences (as defined in Article 10 thereof), may be included in report content where voluntarily submitted by a reporter or entered by the Client. The Processor will not intentionally collect such data outside of Client's instructions.

6. Special Categories of Data (if applicable)

The Processing may involve special categories of Personal Data (as defined in Article 9 of the UK GDPR/EU GDPR) where such data is voluntarily submitted by a reporter or entered by the Client in connection with a hotline report or case file. Ethics Suite does not actively solicit such data but will process it where included in Client Personal Data, solely in accordance with Client's documented instructions. Such special categories may include:

- Personal data revealing racial or ethnic origin
- Personal data revealing political opinions
- Personal data revealing religious or philosophical beliefs
- Personal data revealing trade union membership
- Personal data concerning health
- Personal data concerning sex life or sexual orientation
- Personal data relating to criminal convictions and offences (Article 10)

Ethics Suite will not process genetic data or biometric data for the purpose of uniquely identifying a natural person.

7. Subprocessors and International Data Transfer Mechanisms

Entity Name	Entity Country	Role	Description of Service / Processing Activity	Categories of Personal Data Processed	Transfer Mechanism (for International Transfers)
Amazon Web Services, Inc.	United States	Cloud Infrastructure Provider	Cloud infrastructure and hosting services for the case management platform, including storage and processing of Client Personal Data.	Contact details, user authentication data, case content, and metadata related to platform use.	EU: Standard Contractual Clauses (2021) Modules 2 & 3 with supplementary measures. UK: UK International Data Transfer Addendum. Switzerland: Swiss Addendum to the EU SCCs.
Amazon Web Services EMEA SARL	Ireland	Cloud Infrastructure Provider	Cloud infrastructure and hosting services for the case management platform, including storage and processing of Client Personal Data on servers physically located in Ireland.	Contact details, user authentication data, case content, and metadata related to platform use.	Processing occurs within the EEA. No international transfer.
HubSpot, Inc.	United States	CRM Platform	CRM, marketing automation, and Client communication tools used to manage Client relationships, onboarding, and service communications.	Client contact information (name, email, phone, organization), communication records, and limited account details.	EU: Standard Contractual Clauses (2021) Modules 2 & 3 with supplementary measures. UK: UK International Data Transfer Addendum. Switzerland: Swiss Addendum to the EU SCCs.
Microsoft Corporation (Outlook / Office 365)	United States	Communication and Productivity Platform	Email, calendar, and collaboration tools used for business communications, scheduling, and	Client contact information contained in business correspondence (name, email,	EU: EU–U.S. Data Privacy Framework (adequacy decision, July 2023).

			document management related to Client service and account administration.	phone, organization) and related communication metadata.	UK: UK Extension to the Data Privacy Framework. Switzerland: Swiss–U.S. Data Privacy Framework. Fallback: Standard Contractual Clauses (2021) incorporated in Microsoft’s Online Services DPA.
Commvault Systems, Inc.	United States	Backup and Disaster Recovery Provider	Provides encrypted backup, replication, and recovery services for AWS-hosted and Microsoft 365 environments. Commvault processes encrypted data only and does not have logical access to plaintext Client Personal Data.	Backup copies of Client Personal Data (encrypted), user authentication data, and associated metadata.	EU: Standard Contractual Clauses (2021) Modules 2 & 3 with supplementary measures. UK: UK International Data Transfer Addendum. Switzerland: Swiss Addendum to the EU SCCs.
GoDaddy Operating Company, LLC	United States	Domain, Hosting, and DNS Services Provider	Provides hosting, DNS, and email services for Ethics Suite web properties, including SSL management and domain routing.	IP addresses, form submission metadata, and limited website contact information.	EU: Standard Contractual Clauses (2021) Modules 2 & 3. UK: UK International Data Transfer Addendum. Switzerland: Swiss Addendum to the EU SCCs.

All Subprocessors are bound by written agreements consistent with Article 28 GDPR, the UK Data Protection Act 2018, and the Swiss FADP. Where transfers occur outside the EEA, UK, or Switzerland, appropriate safeguards under Articles 44–50 GDPR (and local equivalents) are implemented.

Exhibit 2

Description of Technical and Organizational Security Measures

Ethics Suite, acting as Processor, will implement and maintain appropriate technical and organizational measures to protect Client Personal Data and to meet its obligations under applicable Data Protection Laws, including Article 32 of the UK GDPR/EU GDPR. Such measures will be designed to ensure a level of security appropriate to the risk and will include, at a minimum:

1. **Disaster Recovery and Backup Resilience**
   Ethics Suite maintains a documented Disaster Recovery and Business Continuity Plan utilizing Commvault Cloud and AWS redundancy, ensuring encrypted backup, geographic replication, and tested restoration procedures. Backups occur multiple times daily across separate AWS Availability Zones, supported by Commvault's anomaly detection and ransomware protection. These procedures are reviewed regularly to ensure rapid recovery and compliance with GDPR Article 32.
2. **Confidentiality and Access Controls**
   a. Informing all personnel with access to Client Personal Data that such data is confidential and subject to contractual and legal protections.
   b. Limiting access to Client Personal Data to personnel who have a need to know for the performance of the Services.
   c. Instructing personnel to access or display Client Personal Data only in secure, non-public locations.
   d. Requiring multi-factor authentication and other available account protection features for systems used to process Client Personal Data.
3. **Device and Storage Security**
   a. Requiring encryption of all devices used to store or transfer Client Personal Data.
   b. Enforcing a strong password policy requiring authentication at initial startup and upon waking from sleep.
   c. Prohibiting the storage of Client Personal Data on portable drives or removable media.
4. **Network and Infrastructure Security**
   a. Protecting servers with firewalls and conducting vulnerability scanning at least biweekly, with remediation of identified issues within 30 days.
   b. Ensuring that Client Personal Data is encrypted in transit and at rest, using encryption methods designed to prevent access by unauthorized third parties (including government agencies without lawful authority).
   c. Applying anonymization or pseudonymization where appropriate, taking into account the nature and purposes of the processing.
5. **Data Transfer Controls**
   a. Transferring Client Personal Data only through unique, randomly generated file-sharing links that automatically expire no later than ten (10) days from creation.
   b. Ethics Suite will review and update these measures periodically to maintain compliance with applicable Data Protection Laws and to address evolving security risks.
6. **Data Subject Rights Assistance**
   Ethics Suite provides reasonable assistance to Clients in fulfilling their obligations to respond to Data Subject requests under applicable Data Protection Laws. Data Subjects may submit requests through Ethics Suite's Data Subject Access Request (DSAR) portal: Privacy Rights Request Form.

Exhibit 3

Standard Contractual Clauses - Controller to Processor

The parties hereby agree that they will comply with the EU Standard Contractual Clauses: Module 2, which are incorporated herein by reference, a copy of which can be found at https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en. The parties agree that the following terms apply:

1. **Clause 7:** The parties have chosen to include Clause 7.

2. **Clause 9(a):** The data importer has the data exporter's general authorisation for the engagement of Subprocessor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of Subprocessors at least 7 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the Subprocessor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

3. **Clause 11(a):** The parties do not incorporate the optional language allowing a Data Subject to lodge a complaint with an independent dispute resolution body at no cost to the Data Subject.

4. **Clause 13(a):** The supervisory authority of one of the Member States in which the Data Subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behavior is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

5. **Clause 17:** These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights.

6. **Clause 18(b):** The parties agree that those shall be the courts of the state in which the Exporter is established.

ANNEX I TO THE STANDARD CONTRACTUAL CLAUSES

A. LIST OF PARTIES

Data exporter(s):

Name:	**Refer to Signatories of the Agreement**
Address:	**Refer to Signatories of the Agreement**
Contact person's name, position and contact details:	**Refer to Signatories of the Agreement**
Activities relevant to the data transferred under these Clauses:	Provide personal information to Ethics Suite to allow for the provision of Services.
Signature and date:	Refer to Signatories of the Agreement
Role (Controller/Processor):	Controller

Data importer(s):

Name:	**Ethics Suite, LLC**
Address:	28150 N Alma School Rd, Suite 103-215, Scottsdale, AZ 85262
Contact person's name, position and contact details:	**Refer to Signatories of the Agreement**
Activities relevant to the data transferred under these Clauses:	The provision of Services to Client
Signature and date:	Refer to Signatories of the Agreement
Role (Controller/Processor):	Processor

B. DESCRIPTION OF TRANSFER

Refer to Exhibit 1 of the DPA.

C. COMPETENT SUPERVISORY AUTHORITY

The competent supervisory authority shall be the authority where the exporter is established.

ANNEX II TO THE STANDARD CONTRACTUAL CLAUSES – TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITYOF THE DATA

A description of the technical and organizational measures implemented by the data importer(s) is set forth in Exhibit 2 of the DPA.

Exhibit 4

UK International Data Transfer Agreement

Part 1: Tables

Table 1: Parties and signatures

Start date	The Effective Date of the Agreement	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Refer to Signatories of the Agreement	**Ethics Suite, LLC.** 28150 N Alma School Rd, Suite 103-215, Scottsdale, AZ 85262
Key Contact	Refer to Signatories of the Agreement	Refer to Signatories of the Agreement
Importer Data Subject Contact	Refer to Signatories of the Agreement	Refer to Signatories of the Agreement
Signatures confirming each party agrees to be bound by this IDTA	Refer to Signatories of the Agreement	Refer to Signatories of the Agreement

Table 2: Transfer Details

UK country's law that governs the IDTA:	☒ England and Wales ☐ Northern Ireland ☐ Scotland
Primary place for legal claims to be made by the Parties	☒ England and Wales ☐ Northern Ireland ☐ Scotland
The status of the Exporter	In relation to the Processing of the Transferred Data: ☒ Exporter is a Controller ☐ Exporter is a Processor or Subprocessor

The status of the Importer	In relation to the Processing of the Transferred Data: ☐ Importer is a Controller ☒ Importer is the Exporter's Processor or Subprocessor ☐ Importer is **not** the Exporter's Processor or Subprocessor (and the Importer has been instructed by a Third Party Controller)
Whether UK GDPR applies to the Importer	☒ UK GDPR applies to the Importer's Processing of the Transferred Data ☐ UK GDPR does not apply to the Importer's Processing of the Transferred Data
Linked Agreement	**If the Importer is the Exporter's Processor or Subprocessor** – the agreement(s) between the parties which sets out the Processor's or Subprocessor's instructions for Processing the Transferred Data: Name of agreement: Data Processing Addendum (the "DPA") Date of agreement: Refer to Signatories of the Agreement. Parties to the agreement: Refer to Signatories of the Agreement. Reference (if any): None. **Other agreements** – any agreement(s) between the parties which set out additional obligations in relation to the Transferred Data, such as a data sharing agreement or service agreement: Name of agreement: N/A Date of agreement: N/A Parties to the agreement: N/A Reference (if any): N/A **If the Exporter is a Processor or Subprocessor** – the agreement(s) between the Exporter and the Party(s) which sets out the Exporter's instructions for Processing the Transferred Data: Name of agreement: N/A Date of agreement: N/A Parties to the agreement: N/A Reference (if any): N/A
Term	The Importer may Process the Transferred Data for the following time period: ☒ the period for which the Linked Agreement is in force ☐ time period: ☐ (only if the Importer is a Controller or not the Exporter's Processor or Subprocessor) no longer than is necessary for the Purpose.

Ending the IDTA before the end of the Term	☒ the parties cannot end the IDTA before the end of the Term unless there is a breach of the IDTA or the parties agree in writing. ☐ the parties can end the IDTA before the end of the Term by serving: months' written notice, as set out in Section 29 (How to end this IDTA without there being a breach).
Ending the IDTA when the Approved IDTA changes	Which parties may end the IDTA as set out in Section 29.2: ☒ Importer ☐ Exporter ☐ neither Party
Can the Importer make further transfers of the Transferred Data?	☒ The Importer MAY transfer on the Transferred Data to another organisation or person (who is a different legal entity) in accordance with Section 16.1 (Transferring on the Transferred Data). ☐ The Importer MAY NOT transfer on the Transferred Data to another organisation or person (who is a different legal entity) in accordance with Section 16.1 (Transferring on the Transferred Data).
Specific restrictions when the Importer may transfer on the Transferred Data	The Importer MAY ONLY forward the Transferred Data in accordance with Section 16.1: ☐ if the Exporter tells it in writing that it may do so. ☐ to: ☒ to the authorised receivers (or the categories of authorised receivers) set out in the DPA. ☐ there are no specific restrictions.
Review Dates	First review date: Effective Date of the DPA The parties must review the Security Requirements at least once: ☐ each month(s) ☐ each quarter ☐ each 6 months ☐ each year ☐ each year(s) ☒ each time there is a change to the Transferred Data, Purposes, Importer Information, TRA or risk assessment, to the extent that Importer is made aware of such changes; Importer will conduct a review at the time of contract renewal

Table 3: Transferred Data

Transferred Data	The personal data to be sent to the Importer under this IDTA consists of that data outlined in Exhibit 1 of the DPA. The categories of Transferred Data will update automatically if the information is updated in the Linked Agreement referred to.
Special Categories of Personal Data and criminal convictions and offences	The Transferred Data includes data relating to that data outlined in Exhibit 1 of the DPA. The categories of special category and criminal records data will update automatically if the information is updated in the Linked Agreement referred to.
Relevant Data Subjects	The Data Subjects of the Transferred Data are those Data Subjects outlined in Exhibit 1 of the DPA. The categories of Data Subjects will update automatically if the information is updated in the Linked Agreement referred to.
Purpose	The Importer may Process the Transferred Data for the purposes set out in the DPA. The purposes will update automatically if the information is updated in the Linked Agreement referred to.

Table 4: Security Requirements

Security of Transmission	As set out in Exhibit 2 of the DPA.
Security of Storage	As set out in Exhibit 2 of the DPA.
Security of Processing	As set out in Exhibit 2 of the DPA.
Organisational security measures	As set out in Exhibit 2 of the DPA.
Technical security minimum requirements	As set out in Exhibit 2 of the DPA.

Updates to the Security Requirements	The Security Requirements will update automatically if the information is updated in the Linked Agreement referred to.

Part 2: Extra Protection Clauses

Extra Protection Clauses:	N/A

Part 3: Commercial Clauses

Commercial Clauses	Commercial Clauses are not used.

Part 4: Mandatory Clauses

Mandatory Clauses	Part 4: Mandatory Clauses of the Approved IDTA, being the template IDTA A.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 5.4 of those Mandatory Clauses.

Exhibit 5

Addendum to the EU SCCs for Transfers Out of Switzerland

In accordance with guidance issued by the Swiss Federal Data Protection and Information Commissioner (**FDPIC**) titled "The transfer of personal data to a country with an inadequate level of data protection based on recognised standard contractual clauses and model contracts," dated 27 August 2021, the parties hereby agree to adopt the standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council annexed to the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021(the "**EU SCCs**") as adapted by this Addendum in order to comply with Swiss legislation and thus be suitable for ensuring an adequate level of protection for data transfers from Switzerland to a third country in accordance with Article 6 paragraph 2 letter a of the Federal Act on Data Protection ("**FADP**").

1. Selected SCCs, Modules and Selected Clauses

The version of the EU SCCs which this Addendum is appended to, detailed below:

Reference (if any): Module 2 of the EU SCCs as set forth in Exhibit 3 of the DPA.

2. Amendments to the EU SCCs

The following amendments are hereby made to the EU SCCs in order for the EU SCCs to comply with Swiss legislation and thus be suitable for ensuring an adequate level of protection for data transfers from Switzerland to a third country in accordance with Article 6 paragraph 2 letter a FADP.

2.1 **Competent supervisory authority in Annex I.C under Clause 13:** The competent supervisory authority shall be the FDPIC, insofar as the data transfer is governed by the FADP; and shall be the EU authority referenced in Annex I.C insofar as the data transfer is governed by the GDPR.

2.2 **Applicable law for contractual claims under Clause 17:** Applicable law for contractual claims under Clause 17 shall be Swiss law or the law of a country that allows and grants rights as a third party beneficiary for contractual claims regarding data transfers pursuant to the FADP; law of an EU member state for those according to the GDPR (free choice for Module 4)

2.3 **Place of jurisdiction for actions between the parties pursuant to Clause 18 b:** Free choice for actions concerning data transfers pursuant to the FADP; court of an EU member state for actions concerning data transfers pursuant to the GDPR.

2.4 **Adjustments or additions concerning the place of jurisdiction for actions brought by Data Subjects**: The term "member state" shall not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c).

2.5 **Adjustments or additions regarding references to the GDPR:** References to the GDPR should be understood as references to the FADP insofar as the data transfers are subject to the FADP.

2.6 **Supplement until the entry into force of the revFADP:** The EU SCCs shall also protect the data of legal entities until the entry into force of the revised FADP.