# Abnormal AI Data Processing Addendum

**Effective May 12, 2025**

---

# Abnormal AI

# Data Processing Addendum

This Data Processing Addendum ("**DPA**") supplements and is incorporated into the **Agreement**.

If the Customer is an Ordering Activity under GSA Schedule Contracts, it shall only be required to comply with the Federal law of the United States and expressly does not agree to comply with any provision of this Data Processing Agreement, EU Law, or law of an EU Member State that is inconsistent with the Federal law of the United States.

**1. Definitions**. The definitions of certain capitalized terms used in this DPA are set forth below. Others are defined in the body of the DPA. Capitalized terms not defined in this DPA are defined in the Agreement.

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

1.2. "**Data Protection Laws**" means all laws and regulations applicable to the Processing of Personal Data under the Agreement, including, as applicable: (i) the California Consumer Privacy Act, as amended by the California Privacy Rights Act, and any binding regulations promulgated thereunder and the California Privacy Rights Act of 2020 (collectively, the "**CCPA/CPRA**"), (ii) the General Data Protection Regulation (Regulation (EU) 2016/679) ("**EU GDPR**" or "**GDPR**"), (iii) the Swiss Federal Act on Data Protection ("**FADP**"), (iv) the EU GDPR as it forms part of the law of England and Wales by virtue of section 3 of the European Union (Withdrawal) Act 2018 (the "**UK GDPR**") and (v) the UK Data Protection Act 2018; in each case, as updated, amended or replaced from time to time.

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

1.4. "**EEA**" means European Economic Area.

1.5. "**Personal Data**" means information about an identified or identifiable natural person or which otherwise constitutes "personal data", "personal information", "personally identifiable information" or similar terms as defined in Data Protection Laws.

1.6. "**Privacy Data Sheet**" means the applicable document, if and when made available on the Abnormal Trust Portal and incorporated by reference into this DPA, that describes the Processing activities in relation to the specific Service supplied to Customer under the Agreement.

1.7. "**Processing**" and inflections thereof refer to any operation or set of operations that is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.8. "**Processor**" means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller.

1.9. "**Restricted Transfer**" means: (i) where EU GDPR applies, a transfer of Personal Data from the EEA to a country outside the EEA that is not subject to an adequacy determination, (ii) where UK GDPR applies, a transfer of Personal Data from the United Kingdom to any country that is not subject to an adequacy determination, or (iii) where FADP applies, a transfer of Personal Data from Switzerland to any country that is not subject to an adequacy determination.

1.10. "**Security Incident**" means any breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data being Processed by Abnormal.

1.11. "**Specified Notice Period**" is 48 hours.

1.12. "**Subprocessor**" means any third party authorized by Abnormal to Process any Personal Data.

1.13. "**Subprocessor List**" means the list of Abnormal's Subprocessors as referred to in Section 4.2 (Subprocessor List) below.

1.14. "**Trust Portal**" means https://security.abnormalsecurity.com/.

**2. Scope and Duration**.

2.1. Roles of the Parties. This DPA applies to Abnormal as a Processor of Personal Data and to Customer as a Controller or Processor of Personal Data.

2.2. Scope of DPA. This DPA applies to Abnormal's Processing of Personal Data under the Agreement to the extent such Processing is subject to Data Protection Laws. This DPA is governed by the governing law of the Agreement unless otherwise required by Data Protection Laws.

2.3. Duration of DPA. This DPA commences on the Agreement Effective Date and terminates upon expiration or termination of the Agreement (or, if later, the date on which Abnormal has ceased all Processing of Personal Data).

2.4. Order of Precedence. Any ambiguity, conflict or inconsistency between this DPA, the Agreement, the Abnormal Information Security Policy, or any other document comprising the Agreement shall be resolved according to the following order of precedence: (1) any Standard Contractual Clauses or other measures to which the Parties have agreed in Schedule 3 (Cross-Border Transfer Mechanisms) or Schedule 4 (Region-Specific Terms), (2) this DPA, (3) the Information Security Policy, (4) the Agreement, and (5) other supplementary documents incorporated into the Agreement. To the fullest extent permitted by Data Protection Laws, any claims brought in connection with this DPA (including its Schedules) will be subject to the terms and conditions, including, but not limited to, the exclusions and limitations, set forth in the Agreement.

**3. Processing of Personal Data**.

3.1. Customer Instructions.

(a) Abnormal will Process Personal Data as a Processor only: (i) in accordance with Customer Instructions, or (ii) to comply with Abnormal's obligations under applicable laws, subject to any notice requirements under Data Protection Laws.

(b) "**Customer Instructions**" means: (i) Processing to provide the Service and as described in the Agreement (including this DPA and the applicable Privacy Data Sheet) and (ii) other reasonable documented instructions of Customer consistent with the terms of the Agreement.

(c) Details regarding the Processing of Personal Data by Abnormal are set forth in Schedule 1 (Subject Matter and Details of Processing) and the applicable Privacy Data Sheet.

(d) Abnormal will notify Customer if it receives an instruction that Abnormal reasonably determines infringes Data Protection Laws (but Abnormal has no obligation to actively monitor Customer's compliance with Data Protection Laws). In such an instance, Abnormal will be entitled to suspend performance of such instruction, until Customer confirms in writing that such instruction is valid under Data Protection Laws.

3.2. Confidentiality.

(a) Abnormal will protect Personal Data in accordance with its confidentiality obligations as set forth in the Agreement.

(b) Abnormal will ensure personnel who Process Personal Data either enter into written confidentiality agreements or are subject to statutory obligations of confidentiality.

3.3. Compliance with Laws.

(a) Abnormal and Customer will each comply with Data Protection Laws in their respective Processing of Personal Data.

(b) Customer will comply with Data Protection Laws in its issuing of Customer Instructions to Abnormal. Customer will ensure that it has established all necessary lawful bases under Data Protection Laws to enable Abnormal to lawfully Process Personal Data for the purposes contemplated by the Agreement (including this DPA), including, as applicable, by obtaining all necessary consents from, and giving all necessary notices to, Data Subjects. Customer is solely responsible for ensuring the accuracy, quality, and legality of Personal Data Processed by Abnormal including the means by which Customer acquired Personal Data.

3.4. Changes to Laws. The Parties will work together in good faith to negotiate an amendment to this DPA as either Party reasonably considers necessary to address the requirements of Data Protection Laws from time to time.

**4. Subprocessors**.

4.1. Use of Subprocessors.

(a) Customer generally authorizes Abnormal to engage Subprocessors to Process Personal Data. Customer further agrees that Abnormal may engage its Affiliates as Subprocessors.

(b) Abnormal will: (i) enter into a written agreement with each Subprocessor imposing data Processing and protection obligations substantially the same as those set out in this DPA and (ii) remain liable for compliance with the obligations of this DPA and for any acts or omissions of a Subprocessor that cause Abnormal to breach any of its obligations under this DPA.

4.2. Subprocessor List. Abnormal will maintain an up-to-date list of its Subprocessors, including their functions and locations, as specified in the Subprocessor List set forth in Schedule 1 or the applicable Privacy Data Sheet.

4.3. Notice of New Subprocessors. Abnormal may update the Subprocessor List from time to time. At least 30 days before any new Subprocessor Processes any Personal Data, Abnormal will add such Subprocessor to the Subprocessor List and notify Customer through email or other means.

4.4. Objection to New Subprocessors.

(a) If, within 30 days after notice of a new Subprocessor, Customer notifies Abnormal in writing that Customer objects to Abnormal's appointment of such new Subprocessor based on reasonable data protection concerns, the Parties will discuss such concerns in good faith.

(b) If the Parties are unable to reach a mutually agreeable resolution to Customer's objection to a new Subprocessor, Customer, as its sole and exclusive remedy, may terminate the Order for the affected Service for convenience and Abnormal will refund any prepaid, unused fees for the terminated portion of the Subscription Term.

**5. Security**.

5.1. Security Measures. Abnormal will implement and maintain reasonable and appropriate technical and organizational measures, procedures and practices, as appropriate to the nature of the Personal Data, that are designed to protect the security, confidentiality, integrity and availability of Personal Data and protect against Security Incidents, in accordance with Abnormal's Security Measures referenced in the Agreement and as further described in Schedule 2 (Technical and Organizational Measures). Abnormal will regularly monitor its compliance with its Security Measures and Schedule 2 (Technical and Organizational Measures).

5.2. Incident Notice and Response.

(a) Abnormal will implement and follow procedures to detect and respond to Security Incidents.

(b) Abnormal will: (i) notify Customer without undue delay and, in any event, not later than the Specified Notice Period, after becoming aware of a Security Incident affecting Customer and (ii) make reasonable efforts to identify the cause of the Security Incident, mitigate the effects and remediate the cause to the extent within Abnormal's reasonable control.

(c) Upon Customer's request and taking into account the nature of the applicable Processing, Abnormal will assist Customer by providing, when available, information reasonably necessary for Customer to meet its Security Incident notification obligations under Data Protection Laws.

(d) Customer acknowledges that Abnormal's notification of a Security Incident is not an acknowledgement by Abnormal of its fault or liability.

(e) Security Incidents do not include unsuccessful attempts or activities that do not compromise the security of Personal Data, including unsuccessful login attempts, pings, port scans, denial of service attacks or other network attacks on firewalls or networked systems.

5.3. Customer Responsibilities.

(a) Customer is responsible for reviewing the information made available by Abnormal relating to data security and making an independent determination as to whether the Service meets Customer's requirements and legal obligations under Data Protection Laws.

(b) Customer is solely responsible for complying with Security Incident notification laws applicable to Customer and fulfilling any obligations to give notices to government authorities, affected individuals or others relating to any Security Incidents.

**6. Data Protection Impact Assessment**. Upon Customer's request and taking into account the nature of the applicable Processing, to the extent such information is available to Abnormal, Abnormal will assist Customer in fulfilling Customer's obligations under Data Protection Laws to carry out a data protection impact or similar risk assessment related to Customer's use of the Service, including, if required by Data Protection Laws, by assisting Customer in consultations with relevant government authorities.

**7. Data Subject Requests**.

7.1. Assisting Customer. Upon Customer's request and taking into account the nature of the applicable Processing, Abnormal will assist Customer by appropriate technical and organizational measures, insofar as possible, in complying with Customer's obligations under Data Protection Laws to respond to requests from individuals to exercise their rights under Data Protection Laws, provided that Customer cannot reasonably fulfill such requests independently (including through use of the Service).

7.2. Data Subject Requests. If Abnormal receives a request from a Data Subject in relation to the Data Subject's Personal Data, Abnormal will notify Customer and advise the Data Subject to submit the request to Customer (but not otherwise communicate with the Data Subject regarding the request except as may be required by Data Protection Laws), and Customer will be responsible for responding to any such request.

**8. Data Return or Deletion**.

8.1. During Subscription Term. During the Subscription Term, Customer may, through the features of the Service or such other means, access, return to itself or delete Personal Data.

8.2. Post Termination.

(a) Following termination or expiration of the Agreement, Abnormal will, in accordance with its obligations under the Agreement, delete all Personal Data from Abnormal's systems.

(b) Deletion will be in accordance with industry-standard secure deletion practices. Abnormal will issue a certificate of deletion upon Customer's request.

(c) Notwithstanding the foregoing, Abnormal may retain Personal Data: (i) as required by Data Protection Laws or (ii) in accordance with its standard backup or record retention policies, provided that, in either case, Abnormal will (x) maintain the confidentiality of, and otherwise comply with the applicable provisions of this DPA with respect to, retained Personal Data and (y) not further Process retained Personal Data except for such purpose(s) and duration specified in such applicable Data Protection Laws.

**9. Audits**.

9.1. Abnormal Records Generally. Abnormal will keep records of its Processing in compliance with Data Protection Laws and, upon Customer's request, make available to Customer any records reasonably necessary to demonstrate compliance with Abnormal's obligations under this DPA and Data Protection Laws.

9.2. Third-Party Compliance Program.

(a) Abnormal will describe its third-party audit and certification programs (if any) and make summary copies of its audit reports (each, an "**Audit Report**") available to Customer upon Customer's written request at reasonable intervals (but not more than once annually) (subject to confidentiality obligations).

(b) Customer may share a copy of Audit Reports with relevant government authorities as required upon their request.

(c) Customer agrees that any audit rights granted by Data Protection Laws will be satisfied by Audit Reports and the procedures of Section 9.3 (Customer Audit) below.

9.3. Customer Audit. Abnormal will make available all information necessary to demonstrate its compliance with data protection policies and procedures implemented as part of the Service. To this end, upon written request (not more than once annually) Customer may, at its sole cost and expense, verify Abnormal's compliance with its data protection obligations as specified in this DPA by: (i) submitting a security assessment questionnaire to Abnormal; and (ii) if Customer is not satisfied with Abnormal's responses to the questionnaire, then Customer may conduct an audit in the form of meetings with Abnormal's information security experts on a mutually agreeable date. Such interviews will be conducted with a minimum of disruption to Abnormal's normal business operations and subject to Abnormal's agreement on scope and timing. Customer may perform the verification described above either itself or by a mutually agreed upon third party auditor, provided that Customer or its authorized auditor executes a mutually agreed upon non-disclosure agreement. Customer will be responsible for any actions taken by its authorized auditor. All information disclosed by Abnormal under this Section 9.3 will be deemed Abnormal Confidential Information, and Customer will not disclose any audit report to any third party except as obligated by law, court order or administrative order by a government agency. Abnormal will remediate any mutually agreed, material deficiencies in its technical and organizational measures identified by the audit procedures described in this Section 9.3 within a mutually agreeable timeframe.

**10. Cross-Border Transfers/Region-Specific Terms**.

10.1. Cross-Border Data Transfers.

(a) Abnormal (and its Affiliates) may Process and transfer Personal Data globally as necessary to provide the Service.

(b) If Abnormal engages in a Restricted Transfer, it will comply with Schedule 3 (Cross-Border Transfer Mechanisms).

10.2. Region-Specific Terms. To the extent that Abnormal Processes Personal Data protected by Data Protection Laws in one of the regions listed in Schedule 4 (Region-Specific Terms), then the terms specified therein with respect to the applicable jurisdiction(s) will apply in addition to the terms of this DPA.

**Schedule 1 – Subject Matter and Details of Processing**

Customer may subscribe in the Trust Portal to receive email notifications with detailed information about certain updates to the processing operations of the Abnormal Service, including as published in the applicable Privacy Data Sheet(s). By clicking on the "Subscribe" link located in the upper right-hand corner of the Trust Portal, Customer will receive an email notification when an update in the Trust Portal is made.

**A. LIST OF PARTIES**

**Data exporter(s):**

| | |
|---|---|
| Name: | The named "Customer" on the signed or accepted Order or Agreement. |
| Address: | The address associated with the Customer on the signed or accepted Order or Agreement. |
| Contact person's name, position and contact details: | The contact details associated with the Customer on the signed or accepted Order or Agreement. |
| Activities relevant to the data transferred under these Clauses: | See Description of Transfer below. |
| Signature and date: | Refer to the signed or accepted Order or Agreement. |
| Role (controller/processor): | Controller |

**Data importer(s):**

| | |
|---|---|
| Name: | Abnormal AI, Inc. |
| Address: | 8474 Rozita Lee Ave, Suite 420, Las Vegas, NV 89113 United States |
| Contact person's name, position and contact details: | The contact details associated with Abnormal on the signed or accepted Order or Agreement. |
| Activities relevant to the data transferred under these Clauses: | See Description of Transfer below. |
| Signature and date: | Refer to the signed or accepted Order or Agreement. |
| Role (controller/processor): | Processor |

**B. DESCRIPTION OF TRANSFER**

| | |
|---|---|
| Categories of data subjects whose personal data is transferred | Individual users of the cloud office applications and infrastructure that Controller has authorized Processor's Service to connect to, including Controller's messaging systems, as well as individuals sending messages to or receiving messages from user accounts. |
| Categories of personal data transferred | • Personal Data contained in message content and file attachments<br>• User information including user name, roles, email, group assignments, and configuration settings<br>• Personal Data contained within activity logs, audit logs, and administrator reports (e.g. user id, IP address)<br><br>More detailed categories of personal data are reflected for the applicable Service as set forth in the applicable Privacy Data Sheets that are made available at the Abnormal Trust Portal. |
| Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures. | N/A |
| The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis). | Ongoing as determined by the Controller. |
| Nature of the processing | Scanning of message contents, files, metadata, activity logs, and cloud application and infrastructure configurations for educational purposes, and identifying and addressing security risks, malicious or other potential loss-inducing activity and signatures.<br><br>More details on Abnormal processing activities of personal data are reflected for the applicable Service as set forth in the applicable Privacy Data Sheets that are made available at the Abnormal Trust Portal. |
| Purpose(s) of the data transfer and further processing. | For the provision of the Service and Support under the Agreement.<br><br>More detailed purposes for Abnormal processing of personal data are reflected for the applicable Service as set forth in the applicable Privacy Data Sheets that are made available at the Abnormal Trust Portal. |
| The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period. | During the Term and as set forth in the data retention policies as published in the Documentation. Additional specific retention periods for Abnormal processing of personal data are reflected for the applicable Service as set forth in the applicable Privacy Data Sheets that are made available at the Abnormal Trust Portal. |

| | |
|---|---|
| For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing. | During the Term and as specified under the Agreement. |

**C. SUBPROCESSORS**

The Controller has authorised the use of the following Subprocessors: The Subprocessors located on the agreed list available at www.abnormalsecurity.com/trust, the Abnormal Trust Portal, and as published in the applicable Privacy Data Sheet.

**Schedule 2 – Technical and Organizational Measures**

Abnormal has taken and will maintain the appropriate administrative, technical, physical and procedural security measures, for the protection of the Personal Data, including the measures set forth below or otherwise made reasonably available by Abnormal. Further up-to-date Service specific technical and organisational measures will be as set out in the applicable Privacy Data Sheets that are made available at the Abnormal Trust Portal.

**Policy Controls:**

- Abnormal has established an information security policy that is reviewed and approved on a regular cadence.
- A framework of security standards has been developed, which supports the objectives of the security policy.
- Procedures and systems exist for requesting, establishing, issuing, suspending, deleting, and closing user accounts and associated access privileges, e.g. system access is granted based upon position, job function, and manager approval.
- Access to Abnormal offices is controlled via card key access, and is under 24/7 CCTV monitoring.
- No Customer Data is stored on Abnormal premises.

**Collection of Data:**

- The Service processes Customer Data on an in-memory basis via API.
- Customer Data that is processed and identified by the Service as security risks, malicious or a loss-inducing activity is transferred to Abnormal servers that support the Service and stored for the period set forth in Abnormal's data retention policies as published in the Documentation. Such data is then automatically deleted at the end of such period.
- All Customer Data is encrypted at rest using multi-factor encryption with a per-file key and AES-256 block cipher, with keys managed by a secured key management service.

**Backup Copies:**

- Procedures for backup and retention of data and programs have been documented and implemented.
- Backups are encrypted and access is limited based upon least privilege.
- Data and programs are backed up regularly and tested to ensure recoverability.

**Computers and Access Terminals:**

- New employees are required to sign a non-disclosure agreement relating to proprietary software and confidentiality of information relating to customers.
- Employees are required to acknowledge receipt of Abnormal's Information Security Policy.
- Access to the production environment is authorized by the appropriate management and is based on least privilege and business need. A multi-factor secure remote access is required for all access to the production systems.
- All print services are disabled by default on all production servers

**Access Controls:**

- All Abnormal employees and contractors are provided with unique userIDs
- Access is only granted to employees whose role requires it.
- Access is disabled upon role reassignment or termination.
- Access is revoked on termination.
- Multi-Factor Authentication, including biometric fingerprint verification, is required to access Abnormal systems and Customer Data.

**Security while transferring and processing:**

- Segmentation of network environment using logical networking controls.
- Default blocked firewall policies.
- Limited number of integration-related endpoints are accessible via public internet and protected by Web Application Firewall (WAFs).
- Public endpoints utilize Application Load Balancers, and are resilient to dynamic changes in query load/throughput
- Data in transit encrypted using TLS 1.2 sessions with a 2048-bit RSA asymmetric key.
- HTTPS required for all web traffic.
- Encrypted connectors for databases using SSL.

**Schedule 3 – Cross-Border Transfer Mechanism**

1. **Definitions**. Capitalized terms not defined in this Schedule are defined in the DPA.

1.1. "**EU Standard Contractual Clauses**" or "**EU SCCs**" means the Standard Contractual Clauses approved by the European Commission in decision 2021/914.

1.2. "**UK International Data Transfer Agreement**" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner, Version B1.0, in force as of March 21, 2022.

1.3. In addition:

| | |
|---|---|
| "**Designated EU Governing Law**" means: | The laws of the Republic of Ireland |
| "**Designated EU Member State**" means: | Republic of Ireland |

2. **EU Transfers**. Where Personal Data is protected by EU GDPR and is subject to a Restricted Transfer, the following applies:

2.1. The EU SCCs are hereby incorporated by reference as follows:

(a) Module 2 (Controller to Processor) applies where Customer is a Controller of Personal Data and Abnormal is a Processor of Personal Data;

(b) Module 3 (Processor to Processor) applies where Customer is a Processor of Personal Data (on behalf of a third-party Controller) and Abnormal is a Processor of Personal Data;

(c) Customer is the "data exporter" and Abnormal is the "data importer"; and

(d) by entering into this DPA, each party is deemed to have signed the EU SCCs (including their Annexes) as of the DPA Effective Date.

2.2. For each Module, where applicable the following applies:

| Section Reference | Selection by the Parties |
|---|---|
| Section I, Clause 7 | The docking clause does not apply. |

| | |
|---|---|
| Section II, Clause 9 | Option 2 will apply, the minimum time period for prior notice of Subprocessor changes shall be as set out in Section 4.3 of this DPA, and Abnormal shall fulfill its notification obligations by notifying Customer of any Subprocessor changes in accordance with Section 4.3 of this DPA. |
| Section II, Clause 11 | The optional language does not apply. |
| Section II, Clause 13 | All square brackets are removed with the text remaining. |
| Section IV, Clause 17 | Option 1 will apply, and the EU SCCs will be governed by the Designated EU Governing Law. |
| Section IV, Clause 18 (b) | Disputes will be resolved before the courts of the Designated EU Member State. |
| Schedule 1 (Subject Matter and Details of Processing) | Contains the information required in Annex 1 of the EU SCCs. |
| Schedule 2 (Technical and Organisational Measures) | Contains the information required in Annex 2 of the EU SCCs. |

2.3. Where context permits and requires, any reference in this DPA to the EU SCCs shall be read as a reference to the EU SCCs as modified in the manner set forth in this Section 2.

**3. Swiss Transfers**. Where Personal Data is protected by the FADP and is subject to a Restricted Transfer, the following applies:

3.1. The EU SCCs apply as set forth in Section 2 (EU Transfers) of this Schedule 3 with the following modifications:

| Section Reference | Selection by the Parties |
|---|---|
| Section II, Clause 13 | The competent supervisory authority shall be the Swiss Federal Data Protection and Information Commissioner. |
| Section IV, Clause 17 (Option 1) | The EU SCCs will be governed by the laws of Switzerland. |
| Section IV, Clause 18 (b) | Disputes will be resolved before the courts of Switzerland. |
| Section IV, Clause 18 (c) | The term Member State must not be interpreted in such a way as to exclude Data Subjects in Switzerland from enforcing their rights in their place of habitual residence in accordance with Clause 18(c). |
| EU GDPR | All references to the EU GDPR in this DPA are also deemed to refer to the FADP. |

**4. UK Transfers**. Where Personal Data is protected by the UK GDPR and is subject to a Restricted Transfer, the following applies:

4.1. The EU SCCs apply as set forth in Section 2 (EU Transfers) of this Schedule 3 with the following modifications:

(a) each party shall be deemed to have signed the "UK Addendum to the EU Standard Contractual Clauses" ("**UK Addendum**") issued by the Information Commissioner's Office under section 119 (A) of the Data Protection Act 2018;

(b) the EU SCCs shall be deemed amended as specified by the UK Addendum in respect of the transfer of Personal Data;

(c) in Table 1 of the UK Addendum, the parties' key contact information is located in Schedule 1 (Subject Matter and Details of Processing) to this DPA;

(d) in Table 2 of the UK Addendum, information about the version of the EU SCCs, modules and selected clauses which this UK Addendum is appended to are located above in this Schedule 3;

(e) in Table 3 of the UK Addendum:

(i) the list of parties is located in Schedule 1 (Subject Matter and Details of Processing) to this DPA;

(ii) the description of transfer is located in Schedule 1 (Subject Matter and Details of Processing) to this DPA;

(iii) Annex II is located in Schedule 2 (Technical and Organizational Measures) to this DPA; and

(iv) the list of Subprocessors is located in Schedule 1 (Subject Matter and Details of Processing) to this DPA.

(f) in Table 4 of the UK Addendum, both the Importer and the Exporter may end the UK Addendum in accordance with its terms (and the respective box for each is deemed checked); and

(g) in Part 2: Part 2 - Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with section 119 (A) of the Data Protection Act 2018 on 2 February 2022, as it is revised under section 18 of those Mandatory Clauses.

**Schedule 4: Region-Specific Terms**

**A. CALIFORNIA**

**1. Definitions**. CCPA/CPRA and other capitalized terms not defined in this Schedule are defined in the DPA.

1.1. "business purpose", "commercial purpose", "personal information", "sell", "service provider" and "share" have the meanings given in the CCPA/CPRA.

1.2. The definition of "Data Subject" includes "consumer" as defined under the CCPA/CPRA.

1.3. The definition of "Controller" includes "business" as defined under the CCPA/CPRA.

1.4. The definition of "Processor" includes "service provider" as defined under the CCPA/CPRA.

**2. Obligations**.

2.1. Customer is providing the Personal Data to Abnormal, acting as a service provider, under the Agreement for the limited and specific business purposes of providing the Service as described in Schedule 1 (Subject Matter and Details of Processing) to this DPA or the applicable Privacy Data Sheet, and otherwise performing under the Agreement.

2.2. Abnormal will comply with its applicable obligations under the CCPA/CPRA and provide the same level of privacy protection to Personal Data as is required by the CCPA/CPRA.

2.3. Abnormal acknowledges that Customer has the right to: (i) take reasonable and appropriate steps under Section 9 (Audits) of this DPA to help to ensure that Abnormal use of Personal Data is consistent with Customer's obligations under the CCPA/CPRA, (ii) receive from Abnormal notice and assistance under Section 7 (Data Subject Requests) of this DPA regarding consumers' requests to exercise rights under the CCPA/CPRA and (iii) upon notice, take reasonable and appropriate steps to stop and remediate unauthorized use of Personal Data.

2.4. Abnormal will notify Customer promptly after it makes a determination that it can no longer meet its obligations under the CCPA/CPRA.

2.5. Absent Customer Instructions or the Customer's prior written agreement, or generating Threat Intelligence, Abnormal will not retain, use or disclose Personal Data: (i) for any purpose, including a commercial purpose, other than the business purposes described in Section 2.1 of this Section A (California) of Schedule 4 and generating Threat Intelligence, or (ii) outside of the direct business relationship between Abnormal with Customer, except, in either case, where and to the extent permitted by the CCPA/CPRA.

2.6. Abnormal will not sell or share Personal Data received under the Agreement.

2.7. Abnormal will not combine Personal Data with other personal information except to the extent a service provider is permitted to do so by the CCPA/CPRA.