Data Processing Addendum – Brave Ads

Last updated: September 9, 2025

1. Purpose and scope

(a) The purpose of this Data Processing Addendum (DPA) is to ensure compliance with applicable legal obligations around the processing of personal data. This DPA reflects the Parties' agreement with respect to the processing of personal data by Brave Software, Inc. (hereinafter, "BSI"). Unless otherwise specified in this Addendum, BSI acts as a processor of personal data on behalf of the controller, as specified in Annex I.

(b) Both Parties listed in Annex I have agreed to this DPA in order to ensure compliance with Applicable Data Protection Laws.

(c) This DPA applies to the processing of personal data as specified in Annex II.

(d) Annexes I to IV are an integral part of this agreement.

(e) This DPA is without prejudice to obligations to which the controller is subject by virtue of other Applicable Data Protection Laws or other legal obligations.

2. Definitions

(a) For purposes of this agreement, the terms "personal data", "processing", "processor", "controller", "data subject", and "sub-processor", shall have the meanings given to them under the EU GDPR or UK GDPR.

(b) The terms "personal information", "business purpose", "service provider", "business", "consumer", and "third party", as defined under Cal. Civ. Code §1798.140, shall be equivalent and interchangeable with the terms defined in point 2(a) of this section.

(c) The term "Applicable Data Protection Laws" shall refer to the following laws:

- EU General Data Protection Regulation, Regulation (EU) 2016/679;
- UK General Data Protection Regulation, Data Protection Act 2018;
- The California Consumer Privacy Act, as amended by the California Privacy Rights Act, the Virginia Consumer Data Protection Act, the Colorado Privacy Act, the Connecticut Data Privacy Act, the Utah Consumer Privacy Act, and other similar data protection laws that may be relevant.

3. Interpretation

(a) This DPA shall be read and interpreted in the light of the provisions of the Applicable Data Protection Laws.

(b) This DPA shall not be interpreted in a way that runs counter to the rights and obligations provided for under the Applicable Data Protection Laws, or in a way that prejudices the fundamental rights or freedoms of the data subjects.

4. Hierarchy

In the event of a contradiction between this DPA and the provisions of related agreements between the Parties existing at the time when this DPA is agreed or entered into thereafter, this DPA shall prevail.

5. Description of the processing activities

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

6. Obligations of the parties

6.1. Instructions

(a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by law of which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

(b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe on Applicable Data Protection Laws.

6.2. Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

6.3. Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Annex II.

6.4. Security of processing

(a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data. In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

(b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

6.5. Sensitive data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

6.6. Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with this DPA and the Applicable Data Protection Laws.

(b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with this DPA.

(c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in this DPA and the Applicable Data Protection Laws. At the controller's request, the processor shall also permit and reasonably contribute to audits of the processing activities covered by this DPA, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.

(d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice. The controller will be limited to one (1) on-site audit in a calendar year. Any on-site audit, whether done by the controller directly, or through a mandated independent auditor, must be done:

> (1) reasonably, in good faith, and in a proportional manner, taking into account the nature and complexity of the services provided;
> (2) with at least four weeks' advance written notice. If an emergency justifies a shorter notice period, the processor will use good faith efforts to accommodate the request; and
> (3) during the processor's normal business hours, under reasonable duration and in a manner that does not unreasonably interfere with the processor's day-to-day operations.

Prior to the commencement of any on-site audit, the Parties shall mutually agree to the scope, time, and duration, and reimbursement rate to the processor, for which the controller shall be solely responsible. Processor shall have the right to reasonably adapt the scope of any on-site Audit to avoid or mitigate risks with respect to, and including, service levels, availability, and confidentiality of other customers' information.

(e) The Parties shall make the information referred to in this Addendum, including the results of any audits, available to the competent supervisory authority/ies on request.

6.7. No sale or sharing of personal information.

(a) The service provider agrees to process data only for the stated business purpose(s) and/or services as described in this DPA. The service provider (and any contracted companies acting on behalf of the service provider) hereby agree, represent, and warrant that it will not:

(1) sell or share personal information a) provided by the business; or b) processed on behalf of the business;
(2) process personal information outside the scope of this relationship (unless required by applicable law);
(3) combine personal information with other personal data or information collected or received from other sources; or
(4) retain, use, or disclose the personal information it receives from the business, or outside the business relationship when collected directly from a consumer, for any other purpose than the business purpose(s) and/or service(s) specified in Annex II of this Addendum, except as otherwise permitted under the Applicable Data Protection Laws.

(b) The service provider certifies that it understands its contractual restrictions as set forth in this clause, and that it shall comply with them.

(c) The service provider shall notify the business if the service provider determines that it can no longer meet its obligations under this Clause 6.7.

6.8. Use of sub-processors

(a) **GENERAL WRITTEN AUTHORISATION:** The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.

(b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with this DPA. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to this DPA and to the Applicable Data Protection Laws.

(c) At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.

(d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.

6.9. International transfers

(a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under laws to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679.

(b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 6.8 for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

7. Assistance to the controller

(a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.

(b) The processor shall reasonably assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions.

(c) In addition to the processor's obligation to assist the controller pursuant to Clause 7(b), the processor shall furthermore reasonably assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

(1) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

(2) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;

(3) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

(4) the obligations in Article 32 Regulation (EU) 2016/679 or other Applicable Data Protection Laws.

(d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

8. Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and reasonably assist the controller for the controller to comply with its obligations under Articles 33 and 34 Regulation (EU) 2016/679 or based on obligations under other applicable laws that the controller is subject, taking into account the nature of processing and the information available to the processor.

8.1. Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall reasonably assist the controller, at the controller's expense:

(a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

(b) in obtaining the following information pursuant to Applicable Data Protection Laws, which shall at least include:

(1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(2) the likely consequences of the personal data breach;

(3) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(c) complying with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

8.2. Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

(a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

(b) the details of a contact point where more information concerning the personal data breach can be obtained;

(c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under the Applicable Data Protection and other relevant laws.

9. Non-compliance with this Addendum and termination

(a) In the event that the processor is in breach of its obligations under this DPA, the controller may instruct the processor to suspend the processing of personal data until the latter complies with this DPA or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with this DPA, for whatever reason.

(b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with this DPA if:

(1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with this DPA is not restored within a reasonable time and in any event within one month following suspension;

(2) the processor is in substantial or persistent breach of this DPA or its obligations under the Applicable Data Protection Laws;

(3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to this DPA or to the Applicable Data Protection Laws.

(c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under this DPA where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 6.1 (b), the controller insists on compliance with the instructions.

(d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with this DPA.

ANNEX I LIST OF PARTIES

Controller(s): [*Identity and contact details of the controller(s), and, where applicable, of the controller's data protection officer]*

1. Name:

Address:

Contact person's name, position and contact details: …

Name of Signatory:

Title/Position:

Signature and accession date:

Processor(s):

Name: **Brave Software, Inc.**

Address: **580 Howard St. Unit 402, San Francisco, CA 94105**

Contact person's name, position and contact details: **Peter Davey, Brave DPO, privacy@brave.com**

Name of Signatory: Bill Engles

Title/Position: CFO

Signature and accession date:

ANNEX II: DESCRIPTION OF THE PROCESSING FOR BRAVE ADS

Nature of Engagement	To provide a managed advertising service	
Summary Description of Services and Purposes of Processing	Brave Software Inc. (the Company) will collect and process personal data necessary to provide the Brave Ads service to the Customer.	
Categories of personal data to be processed	• Full Name • Billing email address(es) • Phone number • Postal Address • Account ID (assigned by Brave) • Other information shared by Customer with the Company (for billing/support queries)	
Categories of Data Subjects	Employees and/or representatives of Advertisers	
Processing activities and lawful basis	Creation & management of accounts	Necessary for the performance of a contract. **Data retained after account closure**: Legitimate interests.
	Operation of the Brave Ads service	Legitimate Interests
	Providing customer support	Necessary for the performance of a contract. User consent
	Optional customer surveys & direct marketing	User consent
	Payments processing	Necessary for the performance of a contract. Legitimate interests.
	Resolving billing queries and troubleshooting	Necessary for the performance of a contract. Legitimate interests.
	To prevent abuse of the Brave Ads platform	Legitimate interests.
	Compliance with the Company's legal obligations	Legal obligation.
Data retention	Data will be held until no longer required to provide the advertising service or to support the resolution of complaints, or where necessary to meet the Company's legal obligations. For account information, data will be held from seven years after termination of the account.	
Frequency of the transfer	Ongoing	
Contact	privacy@brave.com	

ANNEX III TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

As specified by the contractual agreements and data processing addendums signed with our sub-processors.

CONFIDENTIALITY, INTEGRITY, AVAILABILITY AND RESILIENCE OF PROCESSING SYSTEMS AND SERVICES

Technical Measures:

- Regular automated backups of personal data with secure off-site storage
- Disaster recovery systems and infrastructure
- Redundant systems and storage, including failover mechanisms to ensure availability
- Regular system updates, patches, and security maintenance
- Regular testing of backup and recovery procedures
- Network security measures including firewalls
- Secure system architecture and network segmentation
- Implementation of business continuity systems

Organizational Measures:

- Regular security vulnerability management
- Incident escalation and response
- Change management processes for system modifications
- Documented security policies and procedures
- Vendor and third-party security assessment processes
- Documented disaster recovery and business continuity plans
- Regular testing and updating of recovery procedures
- Defined recovery time objectives (RTO) and recovery point objectives (RPO)
- Staff training on emergency response and recovery procedure
- Maintenance contracts and support agreements for critical systems

SECURE TRANSMISSION & STORAGE OF DATA

Technical Measures:

- Encryption of personal data at rest using AES-256 or equivalent encryption standards
- Encryption of data in transit using TLS 1.2 or higher
- Secure file transfer protocols (HTTPS, SSH)
- Virtual private networks (VPN)
- Network security controls and monitoring
- Implementation of pseudonymisation techniques where technically feasible and appropriate
- Secure database management systems with access controls, including the use of encrypted databases and file systems for storing personal data.

Organizational Measures:

- Approved methods for data transfer and communication

- Key management procedures including secure generation, storage, rotation, and disposal
- Data retention and disposal policies
- Vendor agreements for cloud storage services

USER IDENTIFICATION AND AUTHORISATION

Technical Measures:

- Unique user identification and authentication systems
- Role-based access control (RBAC) implementation
- Implementation of access controls and authentication mechanisms (Multi-factor authentication for privileged accounts)
- Session management and timeout controls

Organizational Measures:

- User access management policies and procedures
- Joiner, mover, leaver (JML) procedures
- Segregation of duties and least privilege principles

AUDIT & EVENTS LOGGING

Technical Measures:

- Regular & comprehensive audit logging of system access and activities
- Secure log storage and retention systems
- Log integrity protection and tamper detection
- Automated log analysis and reporting tools
- Logging of security events

Organizational Measures:

- Log management policies and procedures
- Incident response procedures based on log events
- Log retention schedules aligned with legal requirements

SECURE SYSTEMS CONFIGURATION & HARDENING

Technical Measures:

- Automated configuration management and deployment
- Removal of unnecessary services and accounts
- Configuration change detection and alerting

Organizational Measures:

- System configuration management policies
- Change control procedures for system modifications

DATA GOVERNANCE, MANAGEMENT & COMPLIANCE

Technical Measures:

- IT asset management and inventory systems
- Integration of security controls into IT processes
- Updated Records of Processing Activities
- Comprehensive audit trails and logging systems

Organizational Measures:

- Regular management review of IT security measures
- Risk management and assessment processes
- Compliance reporting procedures
- Third party / vendor oversight & review
- Data protection governance processes and procedures
- Data protection & security training
- Documentation of data protection compliance activities
- Transparency in processing

DATA MINIMISATION & STORAGE LIMITATION

Technical Measures:

- Use of privacy-enhancing technologies and techniques including hashing and data minimization
- Privacy by design and default implementation
- Automated data anonymisation and pseudonymisation
- Data usage monitoring and analytics

Organizational Measures:

- Data minimisation policies and procedures
- Data retention policies and schedules
- Privacy by design and default implementation
- Privacy impact assessments for new high-risk processing activities
- Regular review and updating of retention requirements & documentation for processing activities

DATA QUALITY

Technical Measures:

- Data validation and integrity checking systems
- Automated data quality monitoring and reporting
- Version control and change tracking systems
- Error detection and correction mechanisms

Organizational Measures:

- Regular data quality assessments and audits
- Data quality metrics and reporting

TESTING, ASSESSING AND EVALUATING THE EFFECTIVENESS OF TECHNICAL AND ORGANIZATIONAL MEASURES

Technical Measures:

- Automated security scanning and vulnerability assessment tools
- Regular testing of backup and recovery systems
- Continuous monitoring of system performance and availability
- Implementation of certified security controls and products

Organizational Measures:

- Internal audit programs for data protection compliance
- Management oversight & review of security measures and incident reports
- Documentation and tracking of corrective actions
- Documentation of certification processes and results

PHYSICAL SECURITY (AWS)

Technical Measures:

- Access control systems (card readers, biometric systems)
- CCTV surveillance and monitoring systems
- Environmental controls (fire suppression, climate control)
- Secure storage facilities and cabinets
- Secure disposal and destruction of storage media & data
- Intrusion detection and alarm systems
- Backup power systems and surge protection
- Physical security controls for data centers and storage facilities (via AWS)

Organizational Measures:

- Physical security policies and procedures
- Visitor management and escort procedures
- Security personnel and monitoring protocols
- Regular security assessments of physical locations
- Incident response procedures for physical security breaches
- Clear desk and clear screen policies

ANNEX IV: LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors:

Name of Subprocessor	Data Storage Location	Processing Activities	Duration of Processing	Onward Transfer Mechanism	Types of Personal Data Processed
Amazon Web Services	Oregon, United States	Ads account provisioning	Seven years from when an account is terminated.	SCCs	Email address, full name, phone number, Account ID (assigned by Brave).
Stripe	United States	Payments processing	12 months from when an account is deleted.	EU-US Data Privacy Framework / UK-US & CH-US DPFs	A hashed identifier received from Stripe, that links to the account within Stripe system.
Zendesk	United States	Customer support portal for addressing service & billing inquiries	Indefinitely, unless a user makes an erasure request.	SCCs	User ID, user email, IP address, other information provided by user.
Blocksurvey	United States (AWS)	Customer surveys (optional and only occasional data)	The data provided by the user in the survey (1 year via BlockSurvey)	SCCs	Occasionally: user email (most surveys do not include requests for personal data).
Alphabet / Google	United States	Customer support (emails sent to adops@brave.com)	Maximum six years	SCCs	Email address, name, contact information, other information provided by user.
Slack	United States	Internal communications	Slack will process personal data for the duration of the agreement, unless otherwise agreed upon in writing.	Salesforce Processor BCRs / SCCs (UK, Switzerland)	User ID, Account ID
Oracle NetSuite	United States	Invoicing for managed accounts	Returned after contract termination.	Oracle Processor BCRs	Account information, client contact information, billing details.
Ghost.org	Netherlands	Direct marketing / newsletter	Until recipient withdraws consent/opts out	SCCs	Email address
Asana	United States	Inbound inquiries for custom agreements	Asana will retain information for the period necessary	EU-US Data Privacy	Customer prospect information such

			to fulfill the purposes until termination of the agreement.	Framework / UK-US & CH-US DPFs	as name, email address, contact information.
Boostr	United States	Sales Tracking/Advertising management platform & forecasting	Boostr keeps this information as long as necessary to fulfill the purposes outlined in Boostr's Privacy Notice.	SCCs	Customer prospect information.
Twilio (SendGrid)	United States	Transactional emails for self-service accounts	37 days, except for some email event data in pseudonymized form for up to 12 months.	EU-US Data Privacy Framework / Twilio Processor BCRs / SCCs	Email address
Radom	United Kingdom	Crypto payments for self-service ad accounts	Five years	SCCs / Adequacy	Advertisers Wallet Address, and potentially KYC related information

ANNEX V: STANDARD CONTRACTUAL CLAUSES

i. **Location of Processing.** Customer acknowledges that BSI and its sub-processors may transfer and process personal data to and in the United States of America and other locations in which BSI, its Affiliates or its sub-processors maintain data processing operations, as more particularly described in Annex IV. BSI shall ensure that such transfers are made in compliance with Applicable Data Protection Laws and this DPA.

ii. **Transfer Mechanism.** The parties agree that when the transfer of personal data from the Customer (as “data exporter”) to BSI (as “data importer”) is a Restricted Transfer, the Applicable Data Protection Laws require that appropriate safeguards are put in place. For the purposes of such Restricted Transfers from the Customer to BSI, the parties rely on the appropriate Standard Contractual Clauses, which shall be deemed incorporated into and form part of this DPA, as follows:

a. In relation to transfers of Customer personal data that is protected by the GDPR, the EU SCCs shall apply, completed as follows:

1. Module Two or Module Three will apply (as applicable);
2. in Clause 7, the optional docking clause will apply;
3. in Clause 9, Option 2 will apply, and the time period for prior notice of sub-processor changes shall be as set out in Clause 6.8(a) of this DPA;
4. in Clause 11, the optional language will not apply;
5. in Clause 17, Option 1 will apply, and the EU SCCs will be governed by by the law of the EU Member State in which the data exporter is established and if no such law by Irish law;
6. in Clause 18(b), disputes shall be resolved before the courts of the EU Member State in which the data exporter is established and otherwise Ireland;
7. Annex I of the EU SCCs shall be deemed completed with the information set out in Annex 1 to this DPA; and
8. Annex II of the EU SCCs shall be deemed completed with the information set out in Annex III to this DPA.

b. In relation to transfers of personal data protected by the UK GDPR or Swiss DPA, the EU SCCs as implemented under sub-paragraphs (a) and (b) above will apply with the following modifications:

1. references to "Regulation (EU) 2016/679" shall be interpreted as references to UK Data Protection Laws or the Swiss DPA (as applicable);
2. references to specific Articles of "Regulation (EU) 2016/679" shall be replaced with the equivalent article or section of UK Data Protection Laws or the Swiss DPA (as applicable);
3. references to "EU", "Union", "Member State" and "Member State law" shall be replaced with references to "UK" or "Switzerland", or "UK law" or "Swiss law" (as applicable);
4. the term "member state" shall not be interpreted in such a way as to exclude data subjects in the UK or Switzerland from the possibility of suing for their rights in their place of habitual residence (i.e., the UK or Switzerland);
5. Clause 13(a) and Part C of Annex I are not used and the "competent supervisory authority" is the UK Information Commissioner or Swiss Federal Data Protection Information Commissioner (as applicable);
6. references to the "competent supervisory authority" and "competent courts" shall be replaced with references to the "Information Commissioner" and the "courts of England and Wales" or the "Swiss Federal Data Protection Information Commissioner" and "applicable courts of Switzerland" (as applicable);
7. in Clause 17, the Standard Contractual Clauses shall be governed by the laws of England and Wales or Switzerland (as applicable); and

8. with respect to transfers to which UK Data Protection Laws apply, Clause 18 shall be amended to state "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts", and with respect to transfers to which the Swiss DPA applies, Clause 18(b) shall state that disputes shall be resolved before the applicable courts of Switzerland.

c. **UK Savings Clause.** To the extent that and for so long as the EU SCCs as implemented in accordance with sub-paragraphs (a) and (b) above cannot be used to lawfully transfer Customer personal data in accordance with the UK GDPR to BSI, the UK SCCs shall be incorporated into and form an integral part of this DPA and shall apply to transfers governed by the UK GDPR. For the purposes of the UK SCCs, the relevant annexes, appendices or tables shall be deemed populated with the information set out in Annexes I-IV of this DPA.

d. **Application of UK Clauses.** In relation to data that is protected by the UK GDPR, the EU SCCs will apply as follows: (i) apply as completed in accordance with paragraph 7(a) above; and (ii) be deemed amended as specified by Part 2 of the UK Addendum, which shall be deemed incorporated into and form an integral part of this DPA. In addition, Tables 1 and 3 in Part 1 of the UK Addendum shall be completed respectively with the information set out in Annexes I-IV and of this DPA and table 4 in Part 1 of the UK Addendum shall be deemed completed by selecting "neither party".

e. **Hierarchy.** It is not the intention of either party to contradict or restrict any of the provisions set forth in the Standard Contractual Clauses and, accordingly, if and to the extent the Standard Contractual Clauses conflict with any provision of the Agreement (including this DPA) the Standard Contractual Clauses shall prevail to the extent of such conflict.

iii. **Alternative Transfer Mechanism.** To the extent that BSI adopts an alternative data export mechanism (including any new version of or successor to the EU-US Data Privacy Framework or Standard Contractual Clauses adopted pursuant to the Applicable Data Protection Law) (**"Alternative Transfer Mechanism"**), the Alternative Transfer Mechanism shall upon notice to Customer and an opportunity to object, apply instead of any applicable transfer mechanism described in this DPA (but only to the extent such Alternative Transfer Mechanism complies with Applicable Data Protection Laws applicable to Europe and extends to territories to which Customer data is transferred).