

braXos Data Processing Addendum

GDPR / UK GDPR / U.S. State Privacy Law Compliant

Version: 1.0 • Effective Date: September 16, 2026

Contact: privacy@braxos.com

This Data Processing Addendum ("DPA") forms part of and is incorporated into the agreement between braXos Security Software LLC ("braXos," "Processor") and the entity identified in the applicable service agreement ("Customer," "Controller") for the provision of braXos products and services (the "Agreement").

To the extent that braXos processes any Personal Data on the Customer's behalf under the Agreement, the parties agree to comply with the terms of this DPA. In the event of any conflict between this DPA and the Agreement, this DPA shall prevail with respect to the processing of Personal Data.

This DPA is designed to meet the requirements of Article 28 of the GDPR, the UK GDPR, and applicable U.S. state privacy laws, including the CCPA/CPRA, CTDPA, VCDPA, CPA, and other comprehensive state consumer privacy statutes.

1. Definitions

"Applicable Data Protection Law" means all applicable laws and regulations relating to the processing of Personal Data, including the GDPR, UK GDPR, ePrivacy Directive, and applicable U.S. state privacy laws (including the CCPA/CPRA, CTDPA, VCDPA, CPA, and other comprehensive state consumer privacy statutes), in each case as amended, replaced, or superseded from time to time.

"Controller" means the entity that determines the purposes and means of the processing of Personal Data. Under U.S. state privacy laws, this corresponds to a "business" (CCPA/CPRA) or "controller" (CTDPA, VCDPA, CPA, etc.).

"Customer Personal Data" means any Personal Data that braXos processes on behalf of Customer in connection with the provision of the Services under the Agreement.

"Data Subject" means an identified or identifiable natural person to whom Customer Personal Data relates. Under the CCPA/CPRA, this corresponds to a "consumer."

"EEA" means the European Economic Area.

"GDPR" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation).

"Personal Data" means any information relating to an identified or identifiable natural person, as defined under Applicable Data Protection Law. Under the CCPA/CPRA, this corresponds to "personal information."

"Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data.

"Processor" means the entity that processes Personal Data on behalf of the Controller. Under U.S. state privacy laws, this corresponds to a "service provider" (CCPA/CPRA) or "processor" (CTDPA, VCDPA, CPA, etc.).

"Services" means the braXos products and services provided to Customer under the Agreement, including braXpass, Composer, Crescendo, LiftOff, Symphony, Harmony, braXos Maestro, and related services.

"Standard Contractual Clauses" or "SCCs" means the standard contractual clauses for the transfer of personal data to processors established in third countries, as approved by the European Commission (currently Commission Implementing Decision (EU) 2021/914).

"Subprocessor" means any third party engaged by braXos to process Customer Personal Data on braXos's behalf in order to provide the Services.

"UK GDPR" means the GDPR as retained in United Kingdom law by virtue of the European Union (Withdrawal) Act 2018, as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019.

"UK IDTA" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner under Section 119A of the UK Data Protection Act 2018.

2. Scope and Roles of the Parties

2.1 Roles

Customer is the Controller and braXos is the Processor with respect to Customer Personal Data. Where U.S. state privacy laws apply, Customer is the "business" and braXos is the "service provider" (CCPA/CPRA) or equivalent role under other applicable state privacy statutes.

2.2 Scope of Processing

braXos shall process Customer Personal Data only as necessary to provide the Services under the Agreement and as further described in Annex 1 (Details of Processing) of this DPA. braXos shall not process Customer Personal Data for any purpose other than as set forth in the Agreement and this DPA, unless required to do so by Applicable Data Protection Law, in which case braXos shall inform Customer of that legal requirement before processing (unless prohibited by law from doing so).

2.3 Customer Obligations

Customer shall ensure that:

- it has obtained all necessary consents, authorizations, and legal bases required under Applicable Data Protection Law for the processing of Customer Personal Data by braXos;
- its instructions to braXos comply with Applicable Data Protection Law; and

- it has provided all necessary notices to Data Subjects regarding the processing described in this DPA.
-

3. Obligations of braXos as Processor

3.1 Processing Instructions

braXos shall process Customer Personal Data only on documented instructions from Customer, including with regard to transfers of Personal Data to a third country or an international organization, unless braXos is required to do so by Applicable Data Protection Law. In such a case, braXos shall inform Customer of that legal requirement before processing, unless the law prohibits such notification on important grounds of public interest.

3.2 Confidentiality

braXos shall ensure that all persons authorized to process Customer Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. braXos shall ensure that access to Customer Personal Data is limited to those personnel who require such access to perform the Services.

3.3 Security Measures

braXos shall implement and maintain appropriate technical and organizational measures to protect Customer Personal Data against unauthorized or unlawful processing, accidental loss, destruction, or damage. These measures are described in Annex 2 (Technical and Organizational Measures) of this DPA and shall include, at a minimum:

- encryption of Personal Data in transit (TLS 1.2 or higher) and at rest where appropriate;
- measures to ensure ongoing confidentiality, integrity, availability, and resilience of processing systems and services;
- role-based access controls and least-privilege principles;
- multi-factor authentication for administrative access;
- regular testing, assessment, and evaluation of the effectiveness of technical and organizational measures;
- logging, monitoring, and vulnerability management; and
- business continuity and disaster recovery procedures.

braXos shall regularly review and update these measures, taking into account the state of the art, costs of implementation, and the nature, scope, context, and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of Data Subjects.

3.4 Assistance with Data Subject Rights

Taking into account the nature of the processing, braXos shall assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of Customer's obligation to respond to requests for exercising Data Subjects' rights under Applicable Data Protection Law, including rights of access, rectification, erasure, restriction, portability, and objection.

If braXos receives a request from a Data Subject directly, braXos shall promptly redirect the Data Subject to Customer and notify Customer of the request, unless otherwise agreed in writing.

3.5 Assistance with Compliance Obligations

braXos shall assist Customer in ensuring compliance with the following obligations under Applicable Data Protection Law, taking into account the nature of processing and the information available to braXos:

- security of processing (Article 32 GDPR);
- notification of Personal Data Breaches to the supervisory authority (Article 33 GDPR);
- communication of Personal Data Breaches to Data Subjects (Article 34 GDPR); and
- data protection impact assessments and prior consultation with supervisory authorities (Articles 35 and 36 GDPR), where applicable.

4. Personal Data Breach Notification

4.1 Notification

braXos shall notify Customer without undue delay, and in any event within forty-eight (48) hours, after becoming aware of a Personal Data Breach affecting Customer Personal Data. Notification shall be provided to the contact designated by Customer or, absent such designation, to Customer's primary administrative contact.

4.2 Content of Notification

The notification shall include, to the extent reasonably available at the time of notification:

- a description of the nature of the Personal Data Breach, including where possible the categories and approximate number of Data Subjects and Personal Data records concerned;
- the name and contact details of braXos's point of contact for further information;
- a description of the likely consequences of the Personal Data Breach; and
- a description of the measures taken or proposed to be taken to address the Personal Data Breach, including measures to mitigate its possible adverse effects.

4.3 Cooperation

braXos shall cooperate with Customer and take reasonable steps to assist in the investigation, mitigation, and remediation of each Personal Data Breach. braXos shall provide updated information as it becomes available.

4.4 No Assessment by braXos

braXos's obligation to notify Customer of a Personal Data Breach shall not be construed as an acknowledgement of fault or liability by braXos. The assessment of whether a Personal Data Breach requires notification to a supervisory authority or to Data Subjects remains the responsibility of Customer as Controller.

5. Subprocessors

5.1 General Authorization

Customer grants braXos general written authorization to engage Subprocessors to process Customer Personal Data in connection with the provision of the Services. The current list of Subprocessors is set forth in Annex 3 (List of Subprocessors) of this DPA and is also available at braxos.com/legal/subprocessors.

5.2 Notification of Changes

braXos shall notify Customer at least thirty (30) days prior to any intended addition or replacement of a Subprocessor by updating the list at braxos.com/legal/subprocessors and by notifying Customer's designated contact. Customer may subscribe to notifications of Subprocessor changes by emailing privacy@braxos.com.

5.3 Objection Right

Customer may object to the appointment of a new Subprocessor on reasonable data protection grounds by notifying braXos in writing within fifteen (15) days of receiving notice of the proposed change. If Customer objects, braXos shall use commercially reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable alternative. If braXos is unable to provide such alternative within a reasonable period, either party may terminate the affected Services by providing written notice.

5.4 Subprocessor Obligations

braXos shall:

- impose on each Subprocessor, by way of a written contract, data protection obligations no less protective than those set out in this DPA;
- remain fully liable to Customer for the performance of each Subprocessor's obligations; and

- ensure that each Subprocessor agreement includes provisions for the flow-down of equivalent obligations regarding confidentiality, security, breach notification, and data subject rights assistance.
-

6. International Data Transfers

6.1 Transfer Mechanisms

To the extent that the processing of Customer Personal Data involves the transfer of Personal Data from the EEA, the United Kingdom, or Switzerland to a country that has not been recognized as providing an adequate level of data protection, braXos shall ensure that appropriate safeguards are in place, which may include:

- the European Commission's Standard Contractual Clauses (Module 2: Controller to Processor), as set forth in Commission Implementing Decision (EU) 2021/914;
- the UK International Data Transfer Addendum (UK IDTA) issued by the Information Commissioner's Office;
- an adequacy decision by the European Commission, UK Secretary of State, or the Swiss Federal Data Protection and Information Commissioner; or
- any other transfer mechanism approved under Applicable Data Protection Law.

6.2 Standard Contractual Clauses

Where the SCCs apply, the parties agree that:

- braXos is the "data importer" and Customer is the "data exporter";
- Module 2 (Controller to Processor) shall apply;
- the optional docking clause in Clause 7 of the SCCs is included;
- the optional redress mechanism in Clause 11(a) of the SCCs is not included;
- under Clause 9(a), Option 2 (general written authorization) shall apply, with the time period for notice of Subprocessor changes as set forth in Section 5.2 of this DPA;
- under Clause 17, the SCCs shall be governed by the laws of Ireland (or such other EU Member State as agreed in writing); and
- under Clause 18(b), disputes shall be resolved before the courts of Ireland (or such other EU Member State as agreed in writing).

6.3 UK Transfers

For transfers of Customer Personal Data from the United Kingdom, the UK IDTA shall be deemed incorporated into and form part of this DPA. In the event of any conflict between the UK IDTA and this DPA, the UK IDTA shall prevail with respect to UK transfers.

6.4 Supplementary Measures

braXos shall implement supplementary technical and organizational measures where necessary to ensure that the level of protection of Customer Personal Data is not undermined by the transfer, in accordance with guidance issued by the European Data Protection Board or the UK Information Commissioner's Office.

7. Audit Rights

7.1 Information and Audit

braXos shall make available to Customer all information reasonably necessary to demonstrate compliance with this DPA and Article 28 of the GDPR, and shall allow for and contribute to audits, including inspections, conducted by Customer or an independent third-party auditor mandated by Customer.

7.2 Audit Procedure

Audits shall be subject to the following conditions:

- Customer shall provide braXos with at least thirty (30) days' prior written notice of any audit request;
- audits shall be conducted during normal business hours, no more than once per twelve (12) month period (unless required by a supervisory authority or following a Personal Data Breach);
- Customer shall ensure that its auditor is bound by appropriate confidentiality obligations; and
- Customer shall bear its own costs of any audit, unless the audit reveals a material breach of this DPA by braXos.

7.3 Third-Party Certifications

To the extent braXos maintains third-party certifications or audit reports (such as SOC 2 Type II or ISO 27001), braXos shall make summary results or certifications available to Customer upon reasonable request as an alternative to or supplement for on-site audits.

8. Data Retention and Deletion

8.1 Duration of Processing

braXos shall process Customer Personal Data for the duration of the Agreement, unless otherwise agreed in writing or required by Applicable Data Protection Law.

8.2 Return or Deletion

Upon termination or expiration of the Agreement, or upon Customer's written request, braXos shall, at Customer's election:

- return all Customer Personal Data to Customer in a commonly used, machine-readable format; or
- delete all Customer Personal Data from braXos's systems, including from backup and disaster recovery systems, within sixty (60) days of termination.

braXos shall certify in writing that it has complied with this Section upon Customer's request.

8.3 Exceptions

braXos may retain Customer Personal Data to the extent required by Applicable Data Protection Law, provided that braXos shall inform Customer of any such requirement and shall limit the processing of such retained data to the purposes required by law. braXos shall continue to protect such data in accordance with this DPA.

9. U.S. State Privacy Law Provisions

To the extent that U.S. state privacy laws apply to braXos's processing of Customer Personal Data, the following additional provisions shall apply:

9.1 CCPA/CPRA (California)

- braXos is a "service provider" as defined under the CCPA/CPRA and shall process Customer Personal Data only for the specific business purposes set forth in the Agreement and this DPA.
- braXos shall not sell or share (as defined under the CCPA/CPRA) Customer Personal Data.
- braXos shall not retain, use, or disclose Customer Personal Data for any purpose other than for the business purposes specified in the Agreement and this DPA, or as otherwise permitted by the CCPA/CPRA.
- braXos shall not combine Customer Personal Data with personal information that it receives from or on behalf of another person, or that it collects from its own interactions with consumers, except as permitted by the CCPA/CPRA.
- braXos shall assist Customer in responding to verifiable consumer requests, including requests to know, delete, correct, or opt out.
- braXos grants Customer the right to take reasonable and appropriate steps to ensure that braXos uses Customer Personal Data in a manner consistent with Customer's obligations under the CCPA/CPRA.

9.2 Other U.S. State Privacy Laws

Where other U.S. state privacy laws apply (including the CTDPA, VCDPA, CPA, and other applicable statutes), braXos shall:

- process Customer Personal Data only pursuant to the instructions in the Agreement and this DPA;
 - assist Customer in meeting its obligations with respect to consumer rights requests, including access, correction, deletion, portability, and opt-out rights;
 - provide reasonable cooperation and assistance in data protection assessments where required by applicable state law; and
 - comply with applicable requirements regarding confidentiality, security, and limitations on use.
-

10. General Provisions

10.1 Governing Law

This DPA shall be governed by and construed in accordance with the governing law provisions of the Agreement, except to the extent that Applicable Data Protection Law requires otherwise.

10.2 Order of Precedence

In the event of any conflict or inconsistency between this DPA and the Agreement, this DPA shall prevail with respect to the processing of Customer Personal Data. The SCCs (where applicable) shall prevail over all other terms of this DPA to the extent of any conflict.

10.3 Amendments

braXos may update this DPA from time to time to reflect changes in Applicable Data Protection Law, regulatory guidance, or braXos's processing activities. braXos shall notify Customer of material changes at least thirty (30) days in advance. Continued use of the Services after such notice constitutes acceptance of the updated DPA.

10.4 Severability

If any provision of this DPA is found to be invalid or unenforceable, the remaining provisions shall continue in full force and effect, and the invalid or unenforceable provision shall be modified to the minimum extent necessary to make it valid and enforceable.

10.5 Entire Agreement

This DPA, together with the Agreement and any applicable SCCs or UK IDTA, constitutes the entire agreement between the parties with respect to the processing of Customer Personal Data and supersedes all prior discussions, agreements, or understandings on this subject matter.

Annex 1: Details of Processing

The following describes the processing activities carried out by braXos on behalf of Customer.

Element	Description
Subject Matter	Processing of Personal Data in connection with the provision of braXos enterprise physical access control, identity synchronization, workflow automation, vertical transportation, AI-assistant- and MCP-client-mediated access to the customer's connected systems (braXos Maestro), and cloud infrastructure services.
Duration of Processing	The term of the Agreement plus any post-termination retention period described in Section 8 of this DPA.
Nature of Processing	Collection, storage, retrieval, organization, structuring, use, transmission, synchronization, deletion, and destruction of Personal Data as necessary to provide the Services, including identity lifecycle management, credential provisioning and de-provisioning, access group management, elevator call processing, workflow automation, brokering authenticated user requests between an AI assistant or MCP-compatible client and the customer's connected systems of record (braXos Maestro), and audit logging. Maestro processing is stateless with respect to customer content — it brokers requests in real time and does not independently retain the content it processes.
Purpose of Processing	To enable Customer to manage physical access control, identity synchronization, credential management, elevator access, workflow automation, and AI-assistant- or MCP-client-mediated access to Customer's connected systems for Customer's authorized users, buildings, properties, and tenants.
Categories of Data Subjects	Customer's employees, contractors, tenants, visitors, building occupants, and other individuals authorized by Customer to use the Services.
Categories of Personal Data	Name (first and last); email address; phone number (where applicable); device identifiers and IP address; credential information (card number, facility code, credential status, activation/expiration dates); access group membership; elevator call and destination request information; authentication and verification data (including OAuth 2.0 tokens for Maestro); Bluetooth beacon proximity data; request and response content processed transiently through Maestro (which may include personal information residing in Customer's connected systems that the user is authorized to access); connection credentials for connected systems (stored securely, never exposed to the AI model or client); and operational and audit log data.
Sensitive Data (if any)	None intentionally processed. If required in a specific Customer deployment, such processing must be authorized by law and agreed in writing between the parties.

Annex 2: Technical and Organizational Measures

braXos implements and maintains the following technical and organizational security measures to protect Customer Personal Data. These measures are reviewed and updated periodically.

Category	Measures
Encryption	Personal Data encrypted in transit using TLS 1.2 or higher. Encryption at rest applied to databases and storage systems containing Personal Data using AES-256 or equivalent.
Access Control	Role-based access controls (RBAC) with least-privilege principles. Multi-factor authentication (MFA) required for all administrative and privileged access. Unique user accounts for all personnel; no shared credentials. For braXos Maestro: end users authenticate via OAuth 2.0 through the braXos identity service; organization membership is derived server-side; credentials for connected systems are stored securely and applied server-side and are never exposed to the AI model or client.
Network Security	Firewalls, intrusion detection/prevention systems, and network segmentation. Regular vulnerability scanning and penetration testing.
Logging and Monitoring	Centralized logging of access and processing events. Real-time monitoring and alerting for anomalous activity. Log retention in accordance with Applicable Data Protection Law and operational requirements. For Maestro: every request is authenticated, authorized against the user's permissions, and recorded in an audit log.
Personnel Security	Background checks for personnel with access to Customer Personal Data (to the extent permitted by law). Mandatory data protection and security awareness training upon onboarding and annually thereafter. Binding confidentiality obligations for all personnel.
Physical Security	Physical access controls to data center facilities (managed by cloud infrastructure Subprocessors). Access restricted to authorized personnel only.
Incident Response	Documented incident response plan with defined roles, escalation procedures, and notification timelines. Regular testing and review of incident response procedures.
Business Continuity	Regular backups of Customer Personal Data. Disaster recovery procedures with defined recovery time objectives (RTOs) and recovery point objectives (RPOs).
Vendor Management	Due diligence assessment of Subprocessors prior to engagement. Contractual data protection obligations imposed on all Subprocessors. Periodic review of Subprocessor compliance.
Data Minimization	Processing limited to what is necessary for the purposes specified in Annex 1. No processing of Customer Personal Data for braXos's independent purposes. Maestro is stateless with respect to customer content and does not use data to train AI or machine-learning models.
Logical Isolation	Each customer organization is logically isolated within multi-tenant services. For Maestro: a user only reaches data they are authorized to access within their own organization.

Annex 3: List of Subprocessors

The following is the current list of Subprocessors authorized to process Customer Personal Data on braXos's behalf. This list is also maintained at braxos.com/legal/subprocessors and is updated in accordance with Section 5.2 of this DPA.

Subprocessor	Location	Processing Activity	Date Added
Microsoft Azure	United States, Canada, France, Australia, India	Cloud hosting, data storage, compute infrastructure, service performance monitoring, and infrastructure logging and alerting	Sep 16, 2026
Salesforce	United States	Customer support ticketing and communication management	Sep 16, 2026
Google	United States	Transactional email delivery, push notifications, and SMS verification	Sep 16, 2026

Last updated: September 16, 2026

Incorporation

This DPA is incorporated into and forms part of the Agreement. By entering into the Agreement that references this DPA, the parties agree to be bound by its terms with respect to the processing of Customer Personal Data. No separate signature is required.

For customers who entered into the Agreement prior to the effective date of this DPA, the terms of this DPA shall apply from the effective date set forth above. Customers who require an individually executed copy of this DPA may request one by contacting privacy@braxos.com.

braXos Security Software LLC

1-833-4BRAXOS • privacy@braxos.com

7775 Walton Parkway, Suite 100, New Albany, Ohio 43054, USA

131 Finsbury Pavement, London, EC2A 1NS, United Kingdom

© 2026, braXos Security Software LLC. All rights reserved.