

BRANIA

Data Processing Agreement

Version 1.0 | Effective August 7, 2026 | <https://www.brania.ai/legal/dpa>

This Data Processing Agreement ("DPA") forms part of the Master Subscription & Services Agreement and each Order Form that incorporates it. It applies when BRANIA Processes Customer Personal Data on behalf of Customer in connection with the Services.

MEXICO / HEALTH DATA

For a Mexican private-sector Customer, this DPA is intended to address processor/encargado obligations under applicable Mexican private-sector data-protection law, including the Ley Federal de Protección de Datos Personales en Posesión de los Particulares, as amended, together with other applicable data-protection laws. Customer remains responsible as controller/responsible for its privacy notices, legal bases, consents and instructions.

1. Definitions and Roles

"Applicable Data Protection Law" means laws and regulations applicable to the Processing of Customer Personal Data, including, where applicable, Mexican private-sector data-protection law and any other privacy law that applies to the parties' Processing.

"Customer Personal Data" means Personal Data included in Customer Data that BRANIA Processes on Customer's behalf to provide the Services. "Controller" includes equivalent concepts such as responsable; "Processor" includes equivalent concepts such as encargado.

Customer acts as Controller of Customer Personal Data, or as Processor where Customer Processes data on behalf of another Controller. BRANIA acts as Customer's Processor or sub-processor, as applicable, except for limited account, billing, security, legal-compliance or business-contact information BRANIA Processes for its own legitimate business purposes as an independent controller where applicable law recognizes that role.

2. Customer Instructions and Obligations

BRANIA will Process Customer Personal Data only on documented instructions from Customer, including the instructions contained in the Contract Documents and Customer's authorized use/configuration of the Services, unless law requires otherwise. BRANIA will inform Customer if, in BRANIA's reasonable opinion, an instruction would violate Applicable Data Protection Law, unless prohibited by law.

- Customer will provide lawful instructions and will not instruct BRANIA to Process Personal Data in violation of Applicable Data Protection Law.
- Customer is responsible for providing required privacy notices and obtaining required consents or other legal authorization, including for sensitive/health data, call recording, marketing communications, AI processing and international transfers.
- Customer will minimize data submitted to the Services and will not use BRANIA as the authoritative clinical record unless expressly agreed in writing.
- If Customer submits sensitive Personal Data, Customer represents that it has implemented any heightened notice, consent and security requirements applicable to that data.

3. Confidentiality and Personnel

BRANIA will take reasonable steps to ensure that personnel with access to Customer Personal Data have a need to access it, are subject to confidentiality duties and receive appropriate privacy/security awareness for their roles.

4. Security

BRANIA will maintain administrative, technical and organizational safeguards appropriate to the risk, as described in the Security, Hosting & Support Policy at <https://www.brania.ai/legal/security>. BRANIA may rely on security controls of approved infrastructure and service providers. No specific certification is promised unless expressly stated in that policy or an Order Form.

5. Subprocessors

5.1 General Authorization. Customer authorizes BRANIA to use subprocessors necessary to provide the Services, subject to this Section. The current direct Subprocessor List is maintained at <https://www.brania.ai/legal/subprocessors>.

5.2 Requirements. BRANIA will impose written data-protection obligations on each subprocessor that are appropriate to the nature of the Processing and require confidentiality and security protections substantially consistent with this DPA. BRANIA remains responsible for its subprocessors to the extent required by Applicable Data Protection Law.

5.3 Changes. BRANIA may add or replace subprocessors and will update the online list. For a new direct subprocessor expected to materially Process Customer Personal Data, BRANIA will provide reasonable advance notice where practicable. Customer may object in writing on reasonable, documented data-protection grounds. The parties will work in good faith on a commercially reasonable

alternative; if none is reasonably available, BRANIA may terminate the affected feature or Customer may discontinue the affected feature. This does not entitle Customer to terminate unrelated Services or avoid accrued fees.

6. Data Subject / ARCO Requests

Taking into account the nature of Processing, BRANIA will provide commercially reasonable assistance to Customer in responding to valid requests by Data Subjects, including access, rectification, cancellation/deletion, opposition or equivalent rights. If BRANIA receives a request relating to Customer Personal Data, BRANIA will generally direct the requester to Customer unless law requires BRANIA to respond directly.

7. Security Incidents

BRANIA will notify Customer without undue delay after confirming a security incident that results in unauthorized access to, acquisition of, disclosure of, alteration of or destruction of Customer Personal Data for which BRANIA is responsible ("Personal Data Incident"). BRANIA will provide information reasonably available regarding the nature of the incident, affected data, mitigation taken and known contact information, and will reasonably cooperate with Customer's legally required response. Notification is not an admission of fault or liability.

8. Assistance and Compliance Information

BRANIA will provide information reasonably necessary for Customer to demonstrate compliance with Processor-related obligations. Where required by law and not reasonably satisfied by documentation, Customer may request an audit no more than once annually, during normal business hours, on reasonable prior notice, subject to confidentiality and security restrictions. Customer will bear its audit costs and reimburse BRANIA for material time beyond ordinary compliance support unless an audit identifies a material BRANIA breach or is mandated by a regulator due to BRANIA's conduct.

9. International Processing and Transfers

Customer authorizes BRANIA and approved subprocessors to Process and transfer Customer Personal Data in the countries identified in the Subprocessor List to the extent reasonably necessary to provide the Services. The parties will use legally required contractual or other transfer safeguards where Applicable Data Protection Law requires them. Customer remains responsible for ensuring its privacy notices, consents and instructions permit the contemplated transfers. BRANIA will reasonably cooperate with Customer on legally required transfer documentation.

10. Return, Export and Deletion

During the Term, Customer may use available export functionality or request reasonable export assistance subject to the SOW or then-current professional-services rates. After termination, BRANIA will delete or return Customer Personal Data in accordance with Customer's documented request and applicable technical limitations, generally within ninety (90) days after the applicable Service ends, except to the extent data remains in secure backup cycles, is required by law, or is retained solely for legal-defense purposes. Backup copies will remain protected and will not be restored except for disaster recovery or legal necessity.

11. Aggregated and De-identified Data; AI

BRANIA may create aggregated or de-identified data that does not identify Customer or a Data Subject and use it for security, service operations, analytics, benchmarking, research and product improvement. BRANIA will not use identifiable Customer Personal Data to train generalized third-party foundation models unless Customer expressly authorizes that use in writing. AI Processing is further governed by the AI & Automation Terms at <https://www.brania.ai/legal/ai-terms>.

12. Government and Legal Requests

If BRANIA receives a legally binding demand for Customer Personal Data, BRANIA will, where legally permitted, notify Customer and will disclose only the data reasonably required by the demand. BRANIA will not voluntarily provide Customer Personal Data to a governmental authority except where necessary to protect rights, safety or security or as otherwise permitted by law.

13. Liability; Conflict; Term

Liability under this DPA is subject to the limitations and exclusions in the MSA to the maximum extent permitted by Applicable Data Protection Law. This DPA controls over conflicting Contract Documents only with respect to Processing of Customer Personal Data. It remains effective for as long as BRANIA Processes Customer Personal Data for Customer.

14. Online Versioning

The DPA version identified by the applicable Order Form will remain applicable during that Order's Initial Term, except updates required by law or changes that do not materially reduce Customer protections. Material versions will be archived at <https://www.brania.ai/legal/archive>. The Subprocessor List may be updated under Section 5.

Schedule 1 – Details of Processing

Item	Description
Subject matter	Provision of BRANIA Bedrock, Foundation, implementation, support, integrations and related Services.
Nature and purpose	Collection, organization, storage, retrieval, transmission, communications, workflow automation, analytics, prioritization, recommendation generation, support, security and other Processing necessary to provide the Services.
Duration	For the applicable Service Term plus the return/deletion period described in this DPA.
Data subjects	Prospects, patients/customers, leads, Customer employees/contractors, contact-center users, business contacts and other persons whose data Customer submits.
Personal Data	Identity/contact details, communications, appointment/scheduling data, commercial/customer-history data, campaign/source data, operational data, user/account data and other data Customer elects to submit.
Sensitive data	Health-related or other sensitive Personal Data only where expressly contemplated by Customer's configured use, SOW and lawful instructions. Customer must satisfy heightened legal requirements.
Frequency	Ongoing/repeating during Customer's authorized use of the Services.
Direct subprocessors	As maintained at https://www.brania.ai/legal/subprocessors .

Schedule 2 – Minimum Security Categories

- Access control and least-privilege practices appropriate to BRANIA personnel and Customer environments.
- Authentication controls, including multi-factor authentication where supported and appropriate.
- Encryption or secure transport for Customer Personal Data in transit using industry-standard protocols where supported by the applicable platform/provider.
- Encryption-at-rest protections provided by applicable hosted infrastructure/platform services where supported and configured.
- Logging, monitoring and incident-response processes appropriate to the Services and provider capabilities.
- Change management, vulnerability remediation and vendor/security review appropriate to BRANIA's size and risk profile.
- Backup/recovery and resilience mechanisms provided by applicable infrastructure/platform providers, supplemented by BRANIA operational procedures where applicable.
- Confidentiality obligations and access restrictions for personnel and contractors.