Data Protection Agreement

Hermetiq Inc
Version 1.0 | November 6, 2026

This Data Protection Agreement (DPA) governs personal data that Hermetiq processes on a customer's behalf when providing its build intelligence, remote cache, remote execution, and related support services. It supplements the applicable master services agreement, subscription agreement, order form, or other services contract between the parties (Agreement).

The parties are Hermetiq, Inc., a Delaware corporation, at 915 West Foothill Boulevard, Suite C Unit 751, Claremont, CA 91711 (Hermetiq), and the customer identified in the execution details below (Customer). This DPA becomes effective when signed by both parties or incorporated into a binding Agreement. Capitalized terms not defined here have the meanings given in the Agreement.

1 Definitions and interpretation

Applicable Data Protection Law means privacy and data protection laws applicable to a party's processing under this DPA, including, where applicable, the EU General Data Protection Regulation 2016/679 (EU GDPR), the UK GDPR and Data Protection Act 2018, the Swiss Federal Act on Data Protection (Swiss FADP), and applicable United States state privacy laws, including the California Consumer Privacy Act as amended (CCPA).

Customer Personal Data means personal data submitted to the Services by or for Customer, or otherwise received by Hermetiq on Customer's behalf, to provide the contracted services (Services). It includes personal data in build events, logs, profiles, artifacts, prompts, support materials, and hosted user accounts to the extent actually received. Controller, processor, data subject, processing, and personal data have their meanings under Applicable Data Protection Law. References to personal data include personal information under applicable US law.

Personal Data Breach means a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data processed by Hermetiq or a Subprocessor. Subprocessor means a third party engaged by Hermetiq to process Customer Personal Data on Customer's behalf.

2 Roles and deployment boundaries

Customer is the controller and Hermetiq is the processor of Customer Personal Data, except where Customer acts as a processor for another controller, in which case Hermetiq acts as a subprocessor. Customer will obtain the controller's necessary instructions and authorization. Each party will perform the obligations applicable to its role.

For Hermetiq-hosted Services, this DPA applies to Customer Personal Data actually received or processed by Hermetiq in providing the Services. Schedule A describes the processing. Customer selects the data sources, integrations, users, and enabled features within the available configuration.

For an on-premises, self-hosted, or customer-hosted deployment operated entirely within Customer's infrastructure, this DPA does not itself authorize Hermetiq to access, receive, process, transmit, or retain Customer Data. Software installation and use alone create no remote-access or telemetry right. If Customer separately authorizes support access or sends materials containing personal data, the parties must document that access, its purpose, permitted recipients and locations, and retention before it begins. This DPA applies to the personal data Hermetiq then actually processes.

Each party acts independently for its own business contact, invoicing, contracting, and marketing records where it determines the purposes and means of that processing. That limited exclusion does not remove service-account, telemetry, support, or other Customer Personal Data from this DPA merely because Hermetiq also uses similar systems. Hermetiq's independent-controller activities are governed by applicable law and its published privacy policy.

3 Instructions and permitted use

Hermetiq will process Customer Personal Data only on Customer's documented instructions to provide, secure, maintain, and support the contracted Services, including the instructions in this DPA, the Agreement, and Customer's authorized configurations and written requests. The specific purposes and operations are stated in Schedule A. Additional processing or a material change in purpose requires documented instructions and any necessary amendment.

Hermetiq will not sell Customer Personal Data or use it for cross-context behavioral advertising. It will not use Customer Personal Data to train a general-purpose or shared machine-learning model without Customer's separate express written instruction and an appropriate legal basis. No broad improvement, analytics, or license provision in the Agreement overrides these restrictions for Customer Personal Data.

Data is outside this DPA only if it has been anonymized so that it no longer constitutes personal data under Applicable Data Protection Law. Pseudonymized or merely aggregated data that remains personal data stays protected. Any permitted use of genuinely anonymous data must also comply with the Agreement and does not create rights to access data in Customer-hosted deployments.

If law requires processing beyond Customer's instructions, Hermetiq will inform Customer of the legal requirement before processing unless prohibited by law. Hermetiq will immediately inform Customer if, in its opinion, an instruction infringes Applicable Data Protection Law, and may suspend the affected processing while the parties resolve the issue. Customer is responsible for the lawfulness of its instructions, necessary notices and consents, and the accuracy and minimization of data it supplies.

4 Confidentiality and security

Hermetiq will ensure that persons authorized to process Customer Personal Data are bound by confidentiality obligations or an appropriate statutory duty, receive relevant security training, and access data only as needed for their authorized responsibilities.

Hermetiq will implement and maintain appropriate technical and organizational measures to protect Customer Personal Data, considering the nature, scope, context and purposes of processing, risks to individuals, state of the art, and implementation costs. Schedule B sets out the agreed measures. Hermetiq may update measures while maintaining an overall level of protection appropriate to the risk and will not materially reduce agreed protections during the term.

Customer remains responsible for security within infrastructure it operates, user administration, secure configuration, protecting its credentials, and controlling the data it sends. That allocation does not reduce Hermetiq's obligations for processing, access, or systems for which Hermetiq is responsible.

5 Subprocessors

Customer gives general written authorization for the Subprocessors identified in the agreed, deployment-specific register described in Schedule C. Before processing begins, Hermetiq will provide their legal identities, functions, processing countries, applicable transfer safeguards, and the processing entrusted to them. A provider named in a privacy policy is authorized under this DPA only to the extent identified in that agreed register for Customer's Services.

Hermetiq will give Customer at least 30 days' prior written notice of an addition or replacement, including the information needed to assess its data protection implications. Customer may object on reasonable data protection grounds within 15 days of notice. The parties will work in good faith on a reasonable alternative. The proposed Subprocessor will not begin the disputed processing while a timely objection remains unresolved. If no reasonable solution is available, either party may terminate only the affected Services, and Hermetiq will refund prepaid fees for the unused terminated period.

Hermetiq will bind each Subprocessor by a written contract imposing, in substance, the same applicable data protection obligations, and will remain responsible to Customer for its Subprocessors' performance. On request, Hermetiq will provide relevant contractual information, with redactions to protect unrelated confidential information where permitted by law. Changes to processing countries must also satisfy Section 9 and Schedule D.

6 Personal data breaches

Hermetiq will notify Customer without undue delay and in any event within 48 hours after becoming aware of a Personal Data Breach. Initial notice will not be delayed because information is incomplete and will be supplemented as material information becomes available.

To the extent known, notice will describe the nature of the breach, affected data and individuals, likely consequences, measures taken or proposed to contain and remediate it, and a contact for follow-up. Hermetiq will take reasonable steps to contain, investigate, mitigate and remediate the breach, preserve relevant evidence, and reasonably assist Customer with its legal notification obligations.

Customer controls notices concerning its Customer Personal Data to individuals, customers, and authorities unless law requires Hermetiq to notify directly. Hermetiq will coordinate such legally required notice with Customer where permitted. Breach notification is not an admission of fault or liability. Contact details are stated in Schedule A.

7 Requests and regulatory assistance

Taking account of the nature of processing, Hermetiq will assist Customer through appropriate technical and organizational measures with requests to access, correct, delete, restrict, export, or otherwise exercise rights in Customer Personal Data. Hermetiq will promptly forward requests received directly and will not respond substantively without Customer's instructions except where legally required.

Taking account of the information available to it, Hermetiq will assist Customer with security obligations, Personal Data Breach notifications, data protection impact assessments, prior consultation with supervisory authorities, and other assessments or audits required by Applicable Data Protection Law. Hermetiq will make relevant information available and cooperate with competent authorities as required by law.

Hermetiq may charge reasonable, agreed fees for extraordinary assistance outside the ordinary Services, except to remedy its breach or where prohibited by law. Fees or commercial terms will not prevent or delay assistance required by law or applicable transfer clauses.

8 Demonstrating compliance and audits

Hermetiq will maintain appropriate processing records and make available information necessary to demonstrate compliance with this DPA. Customer may first review relevant independent assurance reports, penetration-test summaries, and security documentation under reasonable confidentiality protections.

If those materials do not reasonably establish compliance, Hermetiq will allow and contribute to audits and inspections by Customer or a qualified independent auditor bound by confidentiality. Audits will ordinarily

occur during business hours with reasonable notice, minimize disruption, and protect other customers' data and unrelated confidential information. Routine audits are limited to once in 12 months; that limit and notice requirement do not restrict audits required by law, a competent authority, applicable transfer clauses, or a credible material compliance concern or Personal Data Breach.

The parties will agree reasonable scope and cost arrangements without undermining Customer's legal audit rights. Hermetiq will address identified material noncompliance promptly. Nothing requires disclosure of other customers' personal data or unrestricted production access when secure, effective alternatives permit the required verification.

9 International transfers and government requests

Hermetiq will process Customer Personal Data only in the countries identified in the agreed deployment and Subprocessor register, subject to Customer's instructions and legally required safeguards. Remote access from another country counts as processing there. This DPA does not represent that all processing is confined to a single country.

Before a restricted international transfer occurs, the parties will establish a valid transfer mechanism, complete the necessary transfer details and assessments, and implement required supplementary measures. Schedule D provides the selected EU standard contractual clauses and UK Addendum terms where those instruments are legally applicable. If the selected instrument is unavailable or insufficient for a particular transfer, the parties will put an alternative lawful mechanism in place before that transfer; otherwise the affected transfer will not proceed.

For a legally binding government request for Customer Personal Data, Hermetiq will notify Customer before disclosure unless prohibited, review the request's legality, challenge it where there are reasonable grounds and doing so is legally available, and disclose only the minimum data it is legally required to disclose. Hermetiq will document its assessment and follow the additional obligations in applicable transfer clauses.

10 Return and deletion

At Customer's choice, Hermetiq will return or delete Customer Personal Data within 30 days after termination of the affected Services or Customer's valid written request, and delete existing copies unless law requires retention. Customer must request an export before deletion when it wants data returned. On request, Hermetiq will confirm completion in writing.

Copies in backups that cannot reasonably be deleted individually will be isolated from ordinary use, remain protected by this DPA, and be deleted through the normal backup cycle within 90 days after the deletion request or termination. If a backup is restored, the applicable deletion instructions will be reapplied. Data retained because of a legal requirement will be limited to what the law requires, isolated, and deleted when that requirement ends. Retention exceptions do not permit new commercial use.

These duties apply to data actually held by Hermetiq or its Subprocessors. Customer controls deletion in its own infrastructure; Hermetiq will provide reasonable assistance within the scope of the Services.

11 United States privacy terms

Where the CCPA applies, Customer discloses Customer Personal Data only for the limited, specified business purposes and services in Schedule A, and Hermetiq acts as a service provider or contractor, as applicable. Hermetiq will comply with applicable CCPA obligations and provide the same level of privacy protection required of Customer for that information.

Hermetiq will not sell or share that information; retain, use, or disclose it outside the direct business relationship or for purposes other than the specified services and business purposes; or combine it with

information from another customer or its own consumer interactions except as expressly permitted by the CCPA and implementing regulations. Hermetiq certifies that it understands and will comply with these restrictions.

Customer may take reasonable and appropriate steps to verify that processing is consistent with these obligations, and, upon notice, to stop and remediate unauthorized use. Hermetiq will notify Customer if it determines it can no longer meet these obligations. Subprocessors receiving this information must be bound by the applicable service-provider or contractor requirements. Equivalent processor restrictions and assistance duties apply to the extent required by other applicable US state privacy laws.

12 Priority liability and term

This DPA remains in effect while Hermetiq processes Customer Personal Data. Confidentiality, restrictions on use, deletion obligations, and other provisions intended to survive continue for as long as relevant data is retained.

For conflicts concerning Customer Personal Data, mandatory transfer clauses prevail, followed by this DPA, then the Agreement. An order form overrides this DPA only if it expressly identifies the provision being modified and does not reduce mandatory legal protection. The privacy policy does not amend or expand the processing authorized by this DPA.

The Agreement's liability limits, exclusions, indemnities and remedies apply to this DPA to the extent permitted by law. They do not limit rights of data subjects, mandatory statutory liability, or protections that cannot be limited under applicable transfer clauses. This DPA does not create an independent indemnity or a separate liability cap.

The Agreement's governing law and dispute provisions apply, subject to mandatory law and Schedule D. If the Agreement is silent, California law and the courts of California apply. Amendments to this DPA require both parties' written agreement, except changes to the agreed Subprocessor register under Section 5. Counterparts and legally valid electronic signatures are permitted.

Execution details

Customer legal name _____

Customer registered address _____

Agreement or order form reference _____

Customer privacy and incident notice email _____

Hermetiq privacy and incident contact legal@hermetiq.com

Hermetiq Inc	Customer
Signature _____	Signature _____
Name _____	Name _____
Title _____	Title _____
Date _____	Date _____

Schedule A Processing and transfer details

This schedule describes the Services selected in the Agreement. Customer may narrow the processing by its documented configuration and instructions. The parties must record any additional data categories, recipients, access countries or special requirements before the additional processing starts.

Item	Description
Parties and contacts	Customer is the exporter where applicable; its legal name, address, contact and signature are in the execution details. Hermetiq is the importer and processor or subprocessor; its address and contact are above. Each party's signature or binding incorporation also covers applicable transfer clauses.
Subject matter and purposes	Providing the contracted Bazel build intelligence and analytics, remote cache and remote execution where selected, hosted user access, troubleshooting, security monitoring, and customer support. No unrelated advertising or model-training purpose is authorized.
Operations	Receiving, organizing, storing, querying, analyzing, transmitting, displaying, supporting, returning and deleting data as necessary for the selected Services. Processing may include automated analytics and AI-assisted analysis requested by Customer within those Services.
Data subjects	Customer's authorized users, employees, contractors, developers, administrators and other individuals whose personal data Customer lawfully includes in supplied records or support materials.
Data categories	Names, business contact details and account identifiers; user and device identifiers and IP addresses; repository and commit attribution; build, test, cache, execution and infrastructure metadata; personal data incidentally present in logs, profiles, artifact paths, prompts and support records. Content depends on Customer's enabled data sources.
Sensitive data	The Services are not intended for special-category data, criminal-conviction data, protected health information or payment-card data unless separately agreed in writing with suitable safeguards. Customer will minimize incidental sensitive data. Unexpected receipt remains protected and will be handled under lawful instructions; it does not waive this DPA.
Frequency and duration	Ongoing or event-driven during the Services, and on request for support, followed by the return, deletion and protected retention periods in Section 10.
Deployment and locations	Hosted processing and support locations must be specified in the agreed deployment and Subprocessor register under Schedule C. For customer-hosted deployments, only separately authorized access or data actually supplied is in scope; no automatic remote processing is authorized.

Schedule B Technical and organizational measures

Hermetiq will maintain the following measures for systems and processing it controls. They are contractual requirements for the relevant Services, not a representation that Customer's own environment is operated by Hermetiq. Their implementation will be documented and proportionate to the risks of the processing.

Governance and personnel. Maintain documented security responsibilities, relevant policies, confidentiality obligations, security awareness, and processes for granting and removing access. Review security risks and material changes.

Access control. Use individual identities, least-privilege authorization, strong authentication and multifactor authentication for privileged access. Review access and promptly revoke it when no longer authorized.

Transmission and storage. Protect data in transit with TLS or equivalent secure transport. Encrypt personal data at rest in hosted cloud storage and databases. Protect authentication secrets and cryptographic keys with controlled access and rotation or revocation procedures.

Isolation and infrastructure. Apply logical separation and authorization controls between customer projects and environments, restrict production administrative access, and protect service communications and network boundaries according to the architecture.

Monitoring and vulnerability management. Log relevant security and administrative events, monitor for suspicious activity, assess vulnerabilities, and track risk-based remediation. Conduct security testing appropriate to material risks and changes.

Secure development. Review changes before production deployment, control source and build access, manage dependencies and secrets, and use documented deployment and change-management practices.

Availability and recovery. Maintain appropriate backup, recovery, and continuity procedures for hosted data and critical services; protect backup access and test recovery arrangements periodically according to the risk.

Incidents and privacy requests. Maintain incident response and escalation procedures, investigate Personal Data Breaches, support rights requests, and maintain relevant records. Follow Sections 6 through 8 for notification and assistance.

Minimization and disposal. Limit access, collection and retention to authorized purposes. Support deletion or return, apply protected backup expiry, and use secure disposal methods appropriate to the storage medium.

Supplier oversight and physical security. Review relevant supplier safeguards, impose appropriate contracts, and rely on documented cloud-provider physical and environmental protections for hosted infrastructure.

For support in a customer-controlled environment, access must be time-limited and approved by Customer, use Customer-approved identity and network controls, and avoid copying data outside that environment unless separately authorized. Additional safeguards for sensitive data or a restricted transfer must be documented before the relevant processing.

Schedule C Subprocessors and processing locations

Before Customer Personal Data is processed, the parties will agree a deployment-specific register identifying each applicable provider's exact contracting entity, address, contact, processing function, data categories, processing countries, and transfer safeguards. The register is incorporated into this schedule when provided by Hermetiq and accepted in writing by Customer. New or replacement providers follow Section 5.

The following provider categories are identified in Hermetiq's published privacy policy. They are candidates for the register only where their function actually involves Customer Personal Data for the selected Services. This list alone does not approve unlisted countries or replace the completed register.

Provider	Potential processing for the Services
Google Cloud Google LLC	Hosting, storage, compute, databases and related infrastructure for hosted Services.
Stytch Stytch Inc	Hosted account authentication and session management, including necessary account identifiers and authentication information.
LogRocket LogRocket Inc	Hosted product analytics, diagnostics and session replay where enabled and authorized; scope and data filtering must be recorded.
Google Workspace Google LLC	Business communications and collaboration only to the extent Customer Personal Data is included in authorized support or service communications.

Marketing website analytics, visitor identification, advertising, and sales CRM providers are not authorized to receive Customer Personal Data under this schedule merely because they appear in the public privacy policy. Customer-hosted installations do not transmit Customer Data to these providers under this DPA without separate documented authorization.

Deployment register

Customer and Agreement reference _____

Deployment and primary hosting country _____

Authorized support access countries _____

Register identifier or attached dated register _____

Customer approval and date _____

Each register entry must identify: provider legal name and address; privacy contact; specific operations; data categories; processing and access countries; duration; and applicable transfer mechanism. Unconfirmed processing countries must be completed before the relevant processing or transfer starts. An updated dated register must remain available to Customer.

Schedule D International transfer terms

D1 European Economic Area

Where an EEA transfer of Customer Personal Data to Hermetiq is restricted under the EU GDPR and the following clauses are legally available for that transfer, the standard contractual clauses in the Annex to European Commission Implementing Decision EU 2021/914 of June 4, 2021 (EU SCCs) are incorporated by reference, unmodified except for permitted selections and completion of their appendices. Their official text is available at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj/eng. The parties will retain an accessible copy with the completed transfer record.

Selection	Agreed completion
Applicable module	Module Two where Customer is a controller and Hermetiq is a processor. Module Three where Customer is a processor and Hermetiq is a subprocessor; Customer confirms the upstream controller's instructions and authorization. Only the module applicable to that processing is selected.
Clause 7	The optional docking clause is not included. Additional parties may accede only through a written agreement satisfying the EU SCCs.
Clause 9	Option Two general written authorization applies. Advance notice is 30 days, following Section 5 and the agreed Subprocessor register.
Clause 11	The optional independent dispute-resolution language is not included. Mandatory rights and complaint mechanisms remain available.
Clauses 17 and 18	The law of Ireland governs the EU SCCs and the courts of Ireland are the designated courts, without restricting mandatory data-subject venue rights.
Annex I A	The parties, roles, contact details, activities, and signatures are in the execution details and Schedule A. Customer's role determines the selected module.
Annex I B	Schedule A supplies data subjects, data categories, purpose, nature, frequency, duration, sensitive-data restrictions, and Subprocessor-related processing. The agreed register supplies transfer destinations and entrusted operations.
Annex I C	The competent authority is determined under EU SCC Clause 13: the authority for Customer's EU establishment; otherwise its required EU representative's Member State; otherwise a competent Member State authority where affected data subjects are located. Customer must identify the applicable authority in the transfer record before transfer.
Annex II and Annex III	Schedule B and any agreed supplementary measures supply security details. Schedule C and its completed register supply Subprocessor details. The parties will complete any additional details required for the selected transfer before it begins.

Customer must provide Hermetiq with the identity and contact details of any upstream controller where required for Module Three. Hermetiq will provide reasonable information for the transfer assessment, notify Customer if it can no longer comply, and suspend or terminate the affected transfer as required by the EU SCCs. No provision of the Agreement or this DPA limits the mandatory obligations, remedies or third-party beneficiary rights in the EU SCCs.

D2 United Kingdom

For a UK restricted transfer relying on standard contractual clauses, the ICO International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, Version B1.0 in force March 21, 2022, together with its mandatory clauses as lawfully revised (UK Addendum), is incorporated by reference. Its mandatory terms prevail as required by that instrument. The approved text and completion guidance are available from the Information Commissioner at https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/.

UK Addendum Table 1 is completed by the parties and contacts in the execution details and Schedule A. Table 2 uses the EU SCCs and selections in D1. Table 3 uses Schedule A for Annexes I A and I B, Schedule B for Annex II, and Schedule C with its completed register for Annex III. For Table 4, both the importer and exporter may end the UK Addendum as provided in Section 19 of its mandatory clauses. Mandatory UK adaptations, including applicable law and jurisdiction, apply. The parties will complete the applicable UK transfer assessment and any additional required information before transfer.

D3 Switzerland

For a transfer subject only to the Swiss FADP and requiring contractual safeguards, the EU SCCs apply with references to the EU GDPR understood as references to the Swiss FADP insofar as applicable, the Federal Data Protection and Information Commissioner as the competent supervisory authority, and Swiss law and the courts of Switzerland selected where necessary for those Swiss transfers. References to a Member State do not exclude Swiss data subjects from enforcing rights at their habitual residence where permitted by applicable law. These adaptations do not restrict protections for data also subject to the EU GDPR or UK GDPR.

D4 Transfer record

Applicable exporter role and module _____

Exporter establishment or representative and competent authority _____

Transfer countries and agreed Subprocessor register reference _____

Transfer assessment and supplementary measures reference _____

Customer and Hermetiq approval and date _____

The parties must complete the applicable register and transfer record and verify that the selected safeguards cover the actual processing before any restricted transfer begins. This DPA alone does not establish that any particular recipient is certified under a data privacy framework or that every international transfer is lawful.