

Enterprise Security & Privacy Packet

Public review copy | September 21, 2026

Data processing, AI governance, tenant safeguards, and provider transparency for enterprise procurement.

This packet reproduces the public DPA and governance disclosures. A signed MSA, SOW, BAA, NDA, or DPA controls where terms conflict. It is not an executed agreement, a certification, or authorization to process protected health information.

Zero-retention requirements must be agreed and verified for the specific feature and provider before processing. This packet does not promise universal zero retention or per-tenant encryption keys.

Current policies: <https://bitscaled.tech/legal>

Privacy Policy: <https://bitscaled.tech/legal/privacy>

Terms of Service: <https://bitscaled.tech/legal/terms>

Contract and assurance requests: legal@bitscaled.tech

Privacy requests: privacy@bitscaled.tech

Data Processing Agreement

Version DPA-v2.0 | Effective August 17, 2026

Online source: <https://bitscaled.tech/legal/dpa>

Bitscaled processes Client Data as a processor for managed services and Workspace-hosted client content. The Client is the controller. Website visitor data is covered by the Privacy Policy, not this DPA.

1. Parties and status of this DPA

This Data Processing Agreement ("DPA") is between the customer ("Client," "you") and Bitscaled LLC ("Bitscaled," "we," "us," or "our"), a Florida limited liability company operating from Tampa, United States. It is intended to meet GDPR Article 28 (and equivalent UK GDPR) processor terms when those laws apply to the Client's processing of Client Data.

Note: A signed Master Service Agreement (MSA), Statement of Work (SOW), Business Associate Agreement (BAA), or separately executed DPA controls over this website DPA where they conflict. This page fills gaps when no signed processor addendum exists.

2. Definitions

- "Client Data" means personal data in the Client's systems, tenants, or Workspace-hosted client content that Bitscaled processes to deliver managed services or hosted client content on the Client's instructions.
- "Website Data" means information Bitscaled collects as a controller from visitors, leads, and Bitscaled account users, as described in the Privacy Policy (<https://bitscaled.tech/legal/privacy>).
- "Processing" and "personal data" have the meanings in the GDPR where it applies, and analogous meanings under other privacy laws that apply to the same activity.
- "Subprocessor" means a third party engaged by Bitscaled to process Client Data in connection with the processor services.

3. Roles and what this DPA does not cover

For Client Data, the Client is the controller (or a processor for its own customer) and Bitscaled is the processor. That includes managed IT, cybersecurity, cloud, backup, and related professional services, and client content Bitscaled hosts in Workspace on the Client's instructions.

Website visitor, marketing, and Bitscaled-account data are not processed under this DPA. Bitscaled is the controller for Website Data. See the Privacy Policy (<https://bitscaled.tech/legal/privacy>).

4. Documented instructions

Bitscaled will process Client Data only on documented instructions from the Client, including the MSA, SOW, order, configured product settings, and reasonable written requests, unless EU, UK, or United States law

requires otherwise. If we believe an instruction infringes applicable data-protection law, we will inform the Client when legally permitted.

The Client is responsible for the lawfulness of its instructions, for notices and consents owed to data subjects, and for not instructing Bitscaled to process data outside the contracted scope (including PHI without a signed BAA).

5. Confidentiality

Bitscaled will ensure that persons authorized to process Client Data are bound by confidentiality duties (contract or statute) and will access Client Data only as needed to perform the services or comply with law.

6. Technical and organizational measures

Taking into account the state of the art, cost, nature, scope, context, and purposes of processing, and the risks to individuals, Bitscaled implements the following measures for processor services. This list is what we actually operate. Bitscaled does not claim SOC 2, ISO 27001, PCI DSS, independent pentest, or 24/7 Bitscaled-operated secure data center certification on this page.

- Encryption in transit using TLS for Bitscaled portals and for remote access we control over public networks.
- Encrypted Bitscaled portal sessions (encrypted HTTP-only session cookies).
- Access controls and least-privilege assignment for Bitscaled staff tools.
- Multi-factor authentication on Bitscaled accounts used to deliver the services.
- Operational logging of access and relevant system events.
- Written contracts with vendors that process Client Data, including confidentiality and data-protection terms appropriate to their role.

Note: Hosting, email, and similar vendors apply their own infrastructure controls under their terms. Client-owned tenants (for example Microsoft 365) remain under the Client's contract with that vendor. See Subprocessors (<https://bitscaled.tech/legal/subprocessors>).

7. Subprocessors

The Client authorizes Bitscaled to engage the vendors listed at [/legal/subprocessors](https://bitscaled.tech/legal/subprocessors) (<https://bitscaled.tech/legal/subprocessors>) to process Client Data as needed for the processor services. Optional or environment-gated vendors are used only when the relevant feature, integration, or contract is enabled.

For processor services, the Client may object to a material new subprocessor by emailing legal@bitscaled.tech (<mailto:legal@bitscaled.tech>). We will work in good faith on a commercially reasonable alternative. If we cannot agree, either party may terminate the affected processor services as provided in the MSA or SOW.

8. Assistance with data subject requests

Taking into account the nature of the processing, Bitscaled will assist the Client by appropriate technical and organizational measures, insofar as possible, for the Client to respond to requests from individuals to access, correct, delete, restrict, or port Client Data, or to object to processing (DSAR and similar requests).

If a request is sent to Bitscaled and clearly identifies the Client, we will notify the Client. We will not respond as controller of Client Data unless required by law or expressly instructed by the Client.

9. Personal data breaches

Bitscaled will notify the Client without undue delay after becoming aware of a personal data breach affecting Client Data we process under this DPA, and will provide information reasonably available to us to help the Client meet its own notification duties.

Note: This DPA does not create a hard 72-hour Bitscaled-to-Client notification SLA. Where the GDPR applies, the Client (as controller) may have a 72-hour clock to notify a supervisory authority after becoming aware of a breach. Prompt notice from Bitscaled is intended to help the Client meet that obligation; it is not a guarantee of a fixed processor-to-controller deadline.

10. International transfers

Bitscaled processes Client Data primarily in the United States. Where a restricted transfer of Client Data from the EEA, UK, or Switzerland requires a transfer tool, the parties will rely on the applicable Standard Contractual Clauses (SCCs) and/or the UK International Data Transfer Agreement or Addendum (IDTA), including any module appropriate to processor-to-subprocessor chains.

Execution of this website DPA constitutes the Client's instruction to make such transfers as needed to provide the contracted services, subject to those clauses where required by law.

11. California (CCPA/CPRA)

For Client Data subject to the California Consumer Privacy Act as amended by the CPRA, Bitscaled is a service provider and contractor. Bitscaled will not sell or share Client Data, retain it for any purpose other than the business purpose of performing the services, or combine it with other personal information except as permitted for service providers/contractors.

12. HIPAA and protected health information

This DPA does not cover protected health information (PHI) under HIPAA. Bitscaled is not authorized to create, receive, maintain, or transmit PHI for the Client until a Business Associate Agreement is signed. Do not place PHI in Workspace, tickets, email to Bitscaled, or tools unless that BAA is in place and the SOW includes the work.

13. Description of processing

The following describes the processing of Client Data under this DPA unless a signed SOW or DPA states a narrower or different scope:

Subject matter

Description: Managed IT / MSP support and related professional services, including Workspace-hosted client content when that hosting is in scope.

Duration

Description: The service term in the applicable MSA, SOW, or order, plus limited post-termination retention as described in this DPA.

Nature

Description: Access, storage, and monitoring as needed to perform the contracted services.

Personal data categories

Description: End-user contact details and IT telemetry as instructed by the Client.

Data subjects

Description: The Client's staff and customers, as instructed by the Client.

14. Audits

Bitscaled will make available information reasonably necessary to demonstrate compliance with this DPA. The Client may audit Bitscaled's relevant processor controls on reasonable written notice, during normal business hours, not more than once in any twelve-month period unless a confirmed personal data breach or competent authority requires an additional review.

Audits must avoid unreasonable disruption, protect other customers' confidential information, and may be satisfied in whole or in part by written responses, vendor reports the Client is entitled to receive, or a mutually agreed auditor. The Client bears its own audit costs unless the audit reveals a material breach of this DPA by Bitscaled.

15. Return and deletion

When processor services end, Bitscaled will delete or return Client Data at the Client's choice, except that copies may remain in backups, logs, or archives until they cycle out in the ordinary course, and except where United States or other applicable law requires retention (including legal holds). Residual copies remain subject to this DPA until deleted.

16. Term and conflict

This DPA lasts for the term of the processor services. If a signed MSA, SOW, BAA, or DPA conflicts with this website DPA, the signed document controls for that conflict. Liability for processor services remains subject to the limitations in the Terms of Service (<https://bitscaled.tech/legal/terms>) or the signed MSA, whichever applies.

17. Governing law

This DPA is governed by the laws of the State of Florida, excluding conflict-of-law rules, unless the MSA specifies a different governing law. Venue follows the MSA, or if none, the courts in Hillsborough County, Florida.

18. Contact

Privacy and processor questions go to privacy@bitscaled.tech (<mailto:privacy@bitscaled.tech>) and legal@bitscaled.tech (<mailto:legal@bitscaled.tech>). Use those mailboxes; we have not appointed a statutory DPO and do not use a [dpo@](mailto:dpo@bitscaled.tech) alias.

AI Data Governance

Version AI-GOVERNANCE-2026-09-21 | Effective September 21, 2026

Online source: <https://bitscaled.tech/legal/ai-governance>

How Bitscaled handles Client Data in AI features: no foundation-model training, provider scope, operational retention, and contractual zero-retention requirements.

1. Scope and contract priority

A signed MSA, SOW, BAA, or DPA controls where it conflicts with this summary. The Data Processing Agreement (<https://bitscaled.tech/legal/dpa>) governs Client Data processed on your instructions; the Privacy Policy (<https://bitscaled.tech/legal/privacy>) describes Website Data and account data.

These commitments apply when Bitscaled processes Client Data through an AI feature within the contracted service scope. They do not authorize new processing, change your access permissions, or permit protected health information without a signed BAA.

2. No foundation-model training

Bitscaled does not use Client Data, including customer infrastructure data, telemetry, and source code, to train foundation models. We process that data only on documented client instructions to deliver the agreed services. Operational prompt and tool logs are not used to train public foundation models.

Model-provider processing must stay within the agreed instructions and applicable provider terms. A provider selection alone does not establish a no-training contract for every product, account tier, endpoint, or customer-supplied credential.

3. Provider and feature scope

AI prompts and relevant context may be sent to the model provider configured for a feature. The subprocessor directory (<https://bitscaled.tech/legal/subprocessors>) describes providers and when they are used. Customer-configured integrations and credentials also require review of the customer's agreement with that provider.

- Agree the feature, provider, permitted data categories, processing locations, and retention requirements before submitting regulated or sensitive Client Data.
- Do not include secrets, payment-card data, or PHI unless the specific workflow is contracted and the required safeguards and agreements are in place.
- Review AI output before relying on it. AI processing remains subject to the same company permissions and authorized service scope as the underlying workflow.

4. Operational retention and zero-retention requirements

No training and zero retention are separate commitments. Features may retain saved conversations, workflow inputs and outputs, prompts, tool metadata, and audit records to provide the service, investigate errors, enforce permissions, and prevent abuse. Retention follows the applicable feature settings, Privacy Policy, and signed agreement.

Note: Bitscaled does not provide a universal zero-retention guarantee. A zero-retention commitment requires a signed agreement identifying the feature, provider and endpoint, data covered, provider approval and configuration, and any operational or legal exceptions. Confirm those conditions before sending data that requires zero retention.

Return and deletion of Client Data follow the DPA. Backups, security records, and legally required records may remain for their applicable retention periods; deleting a visible conversation does not promise immediate deletion of every retained copy.

5. Enterprise review

Contact legal@bitscaled.tech (mailto:legal@bitscaled.tech) to document your AI processing requirements in the DPA or SOW. See Data Security and Tenant Boundaries (<https://bitscaled.tech/legal/data-security>) for the controls that support authorized access.

Data Security and Tenant Boundaries

Version DATA-SECURITY-2026-09-21 | Effective September 21, 2026

Online source: <https://bitscaled.tech/legal/data-security>

Bitscaled enterprise security summary covering company-scoped access, row-level security boundaries, encryption, operational audit records, and assurance evidence.

1. Scope and contract priority

A signed MSA, SOW, BAA, or DPA controls where it conflicts with this summary. The Data Processing Agreement (<https://bitscaled.tech/legal/dpa>) governs Client Data processed on your instructions; the Privacy Policy (<https://bitscaled.tech/legal/privacy>) describes Website Data and account data.

This summary describes controls for Bitscaled-operated portals and services. Customer-owned systems and vendor infrastructure follow their own configuration and contracted controls. Service-specific requirements belong in the MSA, SOW, or DPA.

2. Tenant and authorization boundaries

Client Workspace uses authenticated company membership, role-based permissions, and tenant-scoped application queries. Server-side membership checks establish the company context; a company identifier supplied by a caller does not itself grant access.

Admin, Intranet, and Workspace have distinct authorization scopes. Intranet CRM supports Bitscaled internal operations; it is not a separate customer-isolated CRM instance for each Workspace company.

3. Database row-level security

Selected database tables define PostgreSQL row-level security (RLS) policies. RLS coverage is not universal: core identity and CRM access rely on application authorization and tenant filters. Table-owner connections can bypass ordinary RLS, and privileged service-role policies allow broader server access.

Tenant isolation therefore depends on the complete request path: authentication, company membership, permissions, and query scope. An RLS policy in a database schema is not a guarantee that every application connection is constrained by that policy.

4. Encryption and session protection

- Public websites and portals use TLS at the Vercel edge. Remote access that Bitscaled controls over public networks uses TLS.
- Portal session cookies carry an opaque session identifier and use HTTP-only protection, SameSite restrictions, and the Secure flag in production.
- Stored Workspace AI provider credentials use AES-256-GCM application encryption with keys supplied

through server configuration.

- Infrastructure encryption at rest follows the contracted hosting and database services. Credential encryption does not establish a separate cryptographic key for every tenant or imply customer-managed keys for all records.

5. Audit records and operational monitoring

Bitscaled records relevant authentication, access, legal-signature, and workflow events for service operation and investigation. Record contents and retention depend on the feature and applicable agreement. This summary does not promise an immutable record of every action or a single retention period across all services.

Monitoring providers are listed in the subprocessor directory (<https://bitscaled.tech/legal/subprocessors>). Public-site Datadog browser monitoring and optional session replay require analytics consent. AI prompt and workflow retention is described in AI Data Governance (<https://bitscaled.tech/legal/ai-governance>).

6. Assurance and customer evidence

Bitscaled does not claim SOC 2, ISO 27001, PCI DSS, CMMC, or HIPAA certification. Vendor certifications and reports apply only to their stated services, scope, and period; they do not certify Bitscaled or every customer deployment.

Customer-specific evidence belongs in authenticated Workspace or an agreed confidential review. Contact legal@bitscaled.tech (<mailto:legal@bitscaled.tech>) for procurement review, or security@bitscaled.tech (<mailto:security@bitscaled.tech>) to report a security issue. The Security Trust Center (<https://bitscaled.tech/security>) provides the wider operational overview.

Subprocessors

Version SUBPROCESSORS-v1.4 | Effective September 21, 2026

Online source: <https://bitscaled.tech/legal/subprocessors>

Vendors Bitscaled may use to host, deliver, secure, or measure services, including optional and environment-gated providers. Clients may object to material additions used for processor services.

1. About this list

Bitscaled LLC publishes the vendors that may process data in connection with our websites, portals, VaultTools, and contracted processor services. This page wraps our current inventory. It should be read with the Data Processing Agreement (<https://bitscaled.tech/legal/dpa>) and Privacy Policy (<https://bitscaled.tech/legal/privacy>).

Core vendors are used in ordinary provision of the website or processor services. Optional vendors are environment-gated or used only when a product, integration, consent category, or client contract is enabled.

2. Current subprocessors

Vercel Inc.

Role: Hosting

Purpose: Website, application hosting, edge delivery, and cookieless Web Analytics / Speed Insights.

Location: United States

When used: Core

Supabase / PostgreSQL provider

Role: Hosting

Purpose: Primary application database for accounts, CRM, billing, tickets, and legal signatures.

Location: United States

When used: Core

MongoDB (content database)

Role: Hosting

Purpose: Article content and public newsletter subscriber records.

Location: United States

When used: Core

Upstash Redis

Role: Hosting

Purpose: Optional queue, cache, and rate-limit storage when configured.

Location: United States

When used: Optional

Twilio SendGrid

Role: Communications

Purpose: Fallback transactional and marketing email delivery, event webhooks, and inbound parse when SendGrid is configured as the secondary outbound provider.

Location: United States

When used: Optional

Google LLC (reCAPTCHA, optional Maps, optional Gemini)

Role: Security

Purpose: Bot protection on public forms (contact, login, invite accept, VaultSandbox spoof-test); intranet address lookup; optional Gemini draft/image features.

Location: United States

When used: Core

Google Analytics 4

Role: Analytics

Purpose: Public-site usage measurement after analytics cookie consent.

Location: United States

When used: Optional

Datadog, Inc.

Role: Analytics

Purpose: Application monitoring. Browser RUM and session replay on public pages require analytics consent.

Location: United States

When used: Optional

PayPal

Role: Payments

Purpose: Workspace invoice checkout when a client pays an invoice online.

Location: United States

When used: Optional

Microsoft (Microsoft 365 / Graph, optional Entra app)

Role: Productivity

Purpose: Optional Microsoft 365 security snapshot and contracted Microsoft 365 administration.

Location: United States / customer tenant

When used: Optional

Zoom

Role: Communications

Purpose: Optional CRM meeting/phone sync for Bitscaled operations, not public website pages.

Location: United States

When used: Optional

Discord

Role: Operations

Purpose: Optional internal CRM notifications, approval workflows, and Workspace client channels when configured.

Location: United States

When used: Optional

SignalWire

Role: Communications

Purpose: Voice/SMS call flows for contracted clients that use Bitscaled-managed telephony.

Location: United States

When used: Optional

Namecheap VPS / Bitscaled VaultTools host

Role: Hosting

Purpose: Public security tools gateway (vaulttools.bitscaled.tech) and related microservices.

Location: United States

When used: Core

VaultSandbox (email spoof test environment)

Role: Security

Purpose: Authorized SMTP spoof testing for domains the requester is allowed to test.

Location: United States

When used: Optional

Public breach-index lookup

Role: Security

Purpose: Optional exposure checks for emails or domains submitted to Bitscaled security tools.

Location: United States / provider regions

When used: Optional

Apollo, Clay, Lusha, Parallel

Role: Operations

Purpose: Optional B2B CRM enrichment and optional article-automation validation for Bitscaled operations (not Client end-user files unless an SOW says otherwise).

Location: United States

When used: Optional

Resend

Role: Communications

Purpose: Primary transactional and marketing email delivery and event webhooks when Resend is configured.

Location: United States

When used: Core

OpenAI, LLC

Role: Operations

Purpose: Optional Workspace and Intranet AI model provider when configured.

Location: United States

When used: Optional

Anthropic

Role: Operations

Purpose: Optional Workspace and Intranet AI model provider when configured.

Location: United States

When used: Optional

Google Workspace (Gmail, Drive, Calendar, Meet)

Role: Productivity

Purpose: Staff productivity when Bitscaled personnel process Client Data in email, files, scheduling, or meetings. This listing does not claim SOC 2 or HIPAA certification.

Location: United States

When used: Optional

Google Workspace eSignature

Role: Productivity

Purpose: Optional e-sign of MSA, NDA, SOW, BAA, and DPA when configured for a client.

Location: United States

When used: Optional

3. Optional and environment-gated vendors

Optional rows are not "always on." Examples include Redis or queue storage when configured, Google Analytics and Datadog RUM after analytics consent, PayPal checkout when a client pays an invoice online, Microsoft Graph snapshots, Zoom or Discord for Bitscaled operations, SignalWire for contracted telephony, VaultSandbox spoof testing, and breach-lookup providers used by VaultTools.

Vendors currently marked Optional: Upstash Redis; Twilio SendGrid; Google Analytics 4; Datadog, Inc.; PayPal; Microsoft (Microsoft 365 / Graph, optional Entra app); Zoom; Discord; SignalWire; VaultSandbox (email spoof test environment); Public breach-index lookup; Apollo, Clay, Lusha, Parallel; OpenAI, LLC; Anthropic; Google Workspace (Gmail, Drive, Calendar, Meet); Google Workspace eSignature.

4. CRM enrichment vendors

Apollo, Clay, Lusha, and Parallel are used for Bitscaled CRM enrichment of Bitscaled business contacts. They are not used to process the Client's end-user files or customer records as a processor under the DPA unless a signed SOW expressly says otherwise.

5. How to object

If you are a Client whose Client Data we process under the DPA, you may object to a material new subprocessor used for those processor services by emailing legal@bitscaled.tech (mailto:legal@bitscaled.tech). Include your organization name, the vendor, and the reason. We will discuss a commercially reasonable alternative as described in the DPA (<https://bitscaled.tech/legal/dpa>).

6. Updates

We update this page when the inventory changes. The version and effective date on this document identify the published list. Check back here rather than relying on an emailed copy unless your MSA requires a different notice method.

7. Contact

Questions: legal@bitscaled.tech (mailto:legal@bitscaled.tech) or privacy@bitscaled.tech (mailto:privacy@bitscaled.tech).

8. Enterprise vendor assurance

The following directory highlights four infrastructure and communications providers. It supplements the complete inventory above. Jurisdictions reflect the published vendor inventory and are not a contractual guarantee of exclusive data residency.

Vercel Inc.

Service and jurisdiction: Website, application hosting, edge delivery, and cookieless Web Analytics / Speed Insights. Jurisdiction: United States.

When used: Core provider

Certification evidence: Vercel security and compliance (<https://vercel.com/security>)

Scope: Consult Vercel for current certification scope, audit reports, and hosting controls.

Supabase / PostgreSQL provider

Service and jurisdiction: Primary application database for accounts, CRM, billing, tickets, and legal signatures. Jurisdiction: United States.

When used: Core provider

Certification evidence: Supabase security (<https://supabase.com/security>)

Scope: Consult Supabase for current audit reports and controls for the contracted database service.

Twilio SendGrid

Service and jurisdiction: Fallback transactional and marketing email delivery, event webhooks, and inbound parse when SendGrid is configured as the secondary outbound provider. Jurisdiction: United States.

When used: Optional, when configured

Certification evidence: Twilio security overview (<https://www.twilio.com/en-us/legal/security-overview>)

Scope: Confirm that Twilio assurance documents cover the SendGrid services in your agreement.

Datadog, Inc.

Service and jurisdiction: Application monitoring. Browser RUM and session replay on public pages require analytics consent. Jurisdiction: United States.

When used: Optional, when configured

Certification evidence: Datadog security and compliance (<https://www.datadoghq.com/security/>)

Scope: Consult Datadog for current certifications, report access, and monitoring service scope.

Note: These first-party references are a starting point for reviewing certification scope and requesting current reports. Listing a vendor does not verify an active certification for your service or transfer that certification to Bitscaled. Confirm the contracted service, report period, region, and any required BAA with the provider.

9. Change notification requests

Request subprocessor change notifications

(<mailto:legal@bitscaled.tech?subject=Subprocessor%20change%20notification%20request>) from our legal team. Include your organization and the contact address for notices. This opens an email request; it does not automatically subscribe you to a notification service. The notice method and timing follow your signed agreement.

Clients may object to material new subprocessors for processor services as described in DPA section 7 (<https://bitscaled.tech/legal/dpa#subprocessors>). The request does not change the published inventory or authorize a new processing purpose.