How we handle your data (60-second explainer)

Extra Special Technologies, Inc. · Version v2026-09-02 · Effective 2026-09-02

Canonical location of this explainer: `https://hyperlinked.io/legal/data-handling.pdf`

A plain-language, 60-second read. This is the document referred to as the "Customer Data Handling explainer" in our Terms of Service, our Privacy Policy and our Subprocessor List. The legal version is the Privacy Policy, published at `https://hyperlinked.io/legal/privacy.pdf`. Where this explainer and the Privacy Policy differ, the Privacy Policy governs; where this explainer and the Terms of Service differ, the Terms of Service govern.

Where your data lives

Your data lives in **AWS us-west-2 (Oregon, USA)**.

Two of our databases, the ones holding your link configurations and your short links, are also copied to **AWS us-east-1 (N. Virginia, USA)** and **AWS eu-central-1 (Frankfurt, Germany)** so they stay available if a region has problems. Everything else stays in Oregon only, including your account and login records, your organization's members and their roles, the admin audit log, support tickets, analytics, and every file you upload.

Backups. We do not keep a backup in a separate region. Our databases have continuous point-in-time backups covering the last 35 days, kept in the same region as the database itself, and stored files are protected by keeping previous versions in that same region.

EU data. The two replicated databases above are the only customer data copied to Frankfurt, and that copy exists for resilience rather than to provide EU residency. **Primary processing is in the US**, and we do not currently offer EU-only data residency. The full international-transfer disclosures are in the Privacy Policy, and where a Data Processing Agreement applies, its transfer annexes govern.

Our infrastructure provider **AWS** holds SOC 2 Type 2, ISO 27001, and ISO 27018 attestations, available through AWS Artifact (`https://aws.amazon.com/artifact/`). Those are AWS's certifications for the underlying cloud, **not ExtraSpecial's own attestations**.

How it's protected

- **In transit:** industry-standard encrypted transport protocols, currently TLS 1.2 or higher for externally accessible endpoints, with HTTP Strict Transport Security enforced.
- **At rest:** industry-standard encryption, currently including AES-256, with provider-managed key-management controls where applicable.
- **Access and identity:** least-privilege access control. Privileged administrative access uses federated, short-lived credentials and multi-factor authentication. In the product: **multi-factor authentication (TOTP)** with customer-configurable per-organization enforcement, **role-based**

access control with per-tenant data isolation, and **member deprovisioning and off-boarding**.

- **Monitoring and audit:** a **hash-chained audit log of tenant administrative actions**, covering role, access, and billing changes and recording both allowed and denied attempts. That log is archived to an **immutable, write-once store retained for 7 years**. Separately, administrative actions against our own AWS infrastructure are recorded to CloudTrail on two trails: an organization-wide trail retained for **7 years in write-once (Object Lock) storage**, and a per-environment trail retained for 30 days that feeds our real-time alarms. Alarms fire on credential-abuse signals. **Automated security scanning**, covering static analysis, secret scanning, cloud-posture, supply chain, and subdomain takeover, runs on a regular risk-based cadence, with a documented remediation process.

What we log

When you or your audience make requests to the Service, our content-delivery network, object storage, and API gateway write standard access-log records. Those include the requesting **IP address**, the **browser or client user-agent string**, the requested path, and a timestamp. We use them to operate, secure, and troubleshoot the Service.

Two things worth knowing, because they are unusual:

- **Your hyperlink analytics do not carry visitor IP addresses.** The record we ingest for a hyperlink open carries the request's query string, a byte-range indicator, and the matched delivery-path pattern. It carries no IP address, no user-agent string, and no location data.
- **We do not derive visitor location from IP addresses**, except inside a link-preview diagnostic case that you or our support team deliberately opened. Those diagnostic records store a **truncated** IP address rather than the full one, and they expire automatically after 30 days.

Access-log retention is set out in the Privacy Policy retention table. Content-delivery and storage access logs are written to archival storage and do not have an automatic deletion schedule today.

What we don't do

- **We don't sell your data.** Not to data brokers. Not to advertisers. Not to anyone.
- **We don't train AI on your data.** We do not use Your Content to train machine-learning or AI models, neither models we operate nor models operated by our service providers.
- **We don't run third-party ad trackers.** No Google Ads tag. No Meta pixel. No advertising or cross-site tracking cookies.
- **We don't see your card number.** Payments are processed by Stripe (PCI-DSS Level 1) on Stripe-hosted pages. We store only a customer identifier and a subscription identifier.

Who else touches your data

The full list, with the field-by-field detail and a **DPA Subprocessor** column, is published at `https://hyperlinked.io/legal/subprocessors.pdf`. The short version:

- **Amazon Web Services** hosts our cloud infrastructure, meaning compute, storage, identity, and transactional email. It is our one contractual subprocessor for Customer Personal Data.

- **Stripe** processes payments. Payment administration is our own independent-controller activity, so Stripe is not a subprocessor under a customer Data Processing Agreement on its current described use.
- **Google Workspace** hosts our `security@extraspecial.co` mailbox and team email, and receives support-ticket metadata pointers only, meaning organization, ticket number, priority, and a console link, with no ticket subject, body, or message text.
- **GitHub** hosts our source code. No customer data lives there.

Customers with an active Data Processing Agreement receive at least **30 days' prior notice** by email to their designated account, billing, privacy, or notice contact before a new subprocessor begins processing Customer Personal Data, as provided in that agreement. Anyone else can subscribe to those notices by emailing `privacy@extraspecial.co`.

Account and data deletion

Email `privacy@extraspecial.co` to request deletion of your account and content. On confirmation we **remove it from active serving immediately**, and purge stored copies as residual copies age out of our **backup-rotation window, currently approximately 35 days**. Some records are kept longer where the law requires it, namely tax and payment records, data under legal hold, and the immutable administrative audit trail. The full retention schedule is in the Privacy Policy.

We respond to data-subject-rights requests **within one month for GDPR and UK GDPR** requests, extendable by two further months for complex requests, and **within 45 days for CCPA and CPRA** requests, extendable by a further 45 days.

Reporting a security issue

If you spot a vulnerability, email `security@extraspecial.co`. We commit to a **24-hour acknowledgment** and triage within 5 business days. The canonical reporting information is published at `/.well-known/security.txt`, per RFC 9116 (`https://www.rfc-editor.org/rfc/rfc9116.html`).

Compliance posture

ExtraSpecial does not currently hold SOC 2, ISO 27001, or an equivalent independent certification, and does not represent that it does. We rely on the independent certifications and attestations of our infrastructure providers as supporting evidence of their controls, not of ours.

We are working toward SOC 2 as we grow to support enterprise customers, and we already run the practices such a program expects: least-privilege access, multi-factor authentication, automated security scanning, audit logging, and a documented incident-response process. We describe those as practices we follow today, not as a certification we hold. We display no compliance badge we have not earned, and we will publish our status here once there is something independently verifiable to share.