Privacy Policy

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

Controller: Extra Special Technologies, Inc. ("ExtraSpecial", "we", "us", "our"), a Delaware corporation.

Contact: `privacy@extraspecial.co`.

Canonical location of this Privacy Policy: `https://hyperlinked.io/legal/privacy.pdf`

Status of this document. This Privacy Policy is a privacy notice. It describes how ExtraSpecial processes Personal Data as an independent controller. It does not form part of the Terms of Service. Where ExtraSpecial processes Personal Data on a customer's behalf as a processor or subprocessor, that processing is governed by the Data Processing Agreement between ExtraSpecial and that customer, which is available on request to `legal@extraspecial.co`.

1. Scope

This Privacy Policy describes how we collect, use, store, and share Personal Data when you use the ExtraSpecial Service. It applies to the platform at `extraspecial.co`, its APIs, our marketing pages, and any related applications. It does **not** apply to third-party sites or services we link to.

2. Personal data we collect

2.1 Data you provide

- **Account data**: name, email address, password hash (we never see or store your plaintext password), and any profile information you add.
- **Payment data**: billing-address fields and a Stripe customer identifier and subscription identifier. We do **not** receive or store your full payment card number, security code, or expiry date. Payment credentials are collected and stored by Stripe on Stripe-hosted pages under Stripe's own privacy notice (`https://stripe.com/privacy`), and we follow the PCI-DSS SAQ-A path.
- **Your Content**: as defined in the Terms of Service — URL configurations, bookmarks, templates, and other data you submit to the Service. This policy does not redefine the term.
- **Communications**: email, support tickets, or messages you send us.

2.2 Data we collect automatically

- **Service usage**: actions you perform in the Service, for example opening a URL configuration, tied to your account and used for product improvement and support.
- **Web and API access logs**: our content-delivery network, our object storage, and our API gateway write standard access-log records for requests to the Service. Those records include the requesting IP address, the client or browser user-agent string, the requested path, and a timestamp. We use them to operate, secure, and troubleshoot the Service and to reconstruct events during a security investigation. Retention is described in Section 6. We also apply rate limits and managed protection

rules that evaluate the requesting IP address in flight; those evaluations are not kept as a separate record.

- **Hyperlink interaction data**: when someone opens a hyperlink that a customer has configured, we record the interaction so that we can produce the analytics and metered usage information that customer asked for. The record we ingest carries the request's query string, a byte-range indicator, and the matched delivery-path pattern. It does **not** carry the visitor's IP address, user-agent string, or any location data. Where a query string carries an end-user identifier, that identifier is one the customer chose to include; we do not independently resolve it to a named individual.
- **Link-preview diagnostic sessions**: when you or our support team open a diagnostic case to troubleshoot how one of your links previews on a particular platform, we record the requesting client's user-agent string, the requested path, a truncated IP address, and the country, region, and city that our content-delivery network reports for that request. The IP address is truncated before it is stored: for IPv4 the final octet is discarded, and for IPv6 everything after the first three groups is discarded. These records exist only inside a diagnostic case that you or we deliberately opened, and they expire automatically after 30 days.
- **Cookies and similar technologies**: see Section 10.

We do not derive or store approximate location from IP addresses outside a link-preview diagnostic case.

2.3 Data we do NOT collect

- We do **not** use third-party advertising trackers. There is no Google Ads tag, no Meta pixel, and no comparable advertising or cross-site tracking script in the Service or on our marketing pages.
- We do **not** use Your Content to train machine-learning or AI models, neither models we operate nor models operated by our service providers or subprocessors.
- We do **not** sell your Personal Data.

3. How we use personal data

We process Personal Data for the following purposes and legal bases (GDPR Art. 6):

Purpose	Legal basis
Providing the Service to you	Contract (performance of the Terms of Service)
Processing payments	Contract
Securing the Service (fraud, abuse, threat detection)	Legitimate interest (Art. 6(1)(f)), keeping the platform safe
Customer support	Contract; legitimate interest
Product improvement (aggregated analytics)	Legitimate interest, minimal and with no third-party advertising trackers
Legal compliance	Legal obligation, for example tax records and court orders
Marketing communications (opt-in)	Consent (Art. 6(1)(a)), which you may withdraw at any time via the email unsubscribe

4. Sharing, Service Providers and Subprocessors

We disclose Personal Data to service providers and subprocessors that help us operate, secure and support the Service, as described in our public Subprocessor and Infrastructure Vendor List, published at `https://hyperlinked.io/legal/subprocessors.pdf`. A vendor's inclusion on that public list does not necessarily mean that it processes Customer Personal Data as a subprocessor under a Customer Data Processing Agreement.

The principal vendors and the role each plays are:

- **Amazon Web Services (AWS)** hosts the Service's compute, storage, and identity, and sends our transactional email. Primary region: us-west-2 (Oregon, USA). Edge and replica regions: us-east-1 (N. Virginia, USA) and eu-central-1 (Frankfurt, Germany). AWS acts as a subprocessor for Personal Data we process on a customer's behalf. Transactional email includes a **pointer-only** notification ("you have a new reply, view it in the console") sent to a ticket submitter when a support agent replies; that email carries no ticket content.
- **Stripe** processes payments and holds cardholder data. We hold only a customer identifier and a subscription identifier. Payment administration is our own independent-controller activity rather than processing carried out on a customer's behalf.
- **Google Workspace** hosts our `security@extraspecial.co` and team email, and receives support-ticket **metadata pointers** (organization, ticket number, priority, and a console link, with **no ticket subject, body, or message text**) as a chat notification when a ticket is opened or closed.

We do **not** share Personal Data with any other third party except (a) with your consent, (b) as part of a corporate transaction such as a merger or acquisition, with continuing privacy commitments, (c) to comply with valid legal process, or (d) to protect the rights, safety, or property of ExtraSpecial or others.

5. International transfers

Personal Data is stored in **AWS us-west-2 (Oregon, USA)**. Two databases, holding link configurations and short links, are additionally replicated to **AWS us-east-1 (N. Virginia, USA)** and **AWS eu-central-1 (Frankfurt, Germany)** for availability and regional failover. No other data store is replicated outside us-west-2, and in particular the identity directory, organization membership and role records, the administrative audit log, support records, analytics data, and all stored files and assets are held in us-west-2 only.

We do not operate a separate backup region. Backups are AWS point-in-time continuous backups retained in the same region as the database they protect, and stored files are protected by object versioning in the same region. Neither us-east-1 nor eu-central-1 is a backup region.

Primary processing is in the United States; we do not currently offer EU-only data residency.

This policy describes ExtraSpecial's own processing as an independent controller. For transfers of that Personal Data from the EEA, the United Kingdom, or Switzerland to the United States, we rely on the transfer terms in our infrastructure providers' agreements, including the European Commission's Standard Contractual Clauses and, where a transfer is governed by UK law, the ICO International Data Transfer Addendum, as incorporated into those agreements.

Where we process Personal Data on a customer's behalf as a processor or subprocessor, the transfer mechanism, the selected Standard Contractual Clauses modules, and the associated annexes are set out in the Data Processing Agreement with that customer.

EEA, UK, and Swiss data subjects may contact `privacy@extraspecial.co` to request a copy of the clauses governing a transfer of their data.

6. Retention

Data	Retention
Account data	While the account is active. On deletion it is removed from active serving immediately and purged as residual copies age out of our backup-rotation window, currently approximately 35 days, except records the law requires us to keep.
Your Content	While the account is active. On deletion it is removed from active serving immediately and purged as residual copies age out of our backup-rotation window, currently approximately 35 days, except records the law requires us to keep.
Payment records	7 years, for tax and audit obligations. This covers invoices, the monthly usage totals they are billed from, and the daily records that substantiate those totals. The per-job usage detail underneath a charge is kept for 25 months.
Access logs (content delivery and storage)	Written to archival storage for security investigation and incident reconstruction. No automatic deletion schedule is applied to these archived records today.
Access logs (API gateway)	30 days.
Link-preview diagnostic case events	30 days, by automatic expiry.
Administrative audit trail	7 years, held in immutable write-once storage.
Backups	Point-in-time recovery for approximately 35 days, retained in the same region as the database it protects, plus object versioning for stored files in that same region. We do not take periodic snapshots and we do not operate a separate backup region.
Support tickets	Open tickets: while the account is active. Closed tickets: 2 years from close, by automatic expiry, then deleted. Deleting an organization purges that organization's tickets. You may request erasure of the tickets you submitted at any time (Section 7); we delete the whole ticket, meaning your messages, our replies, and the status events.
Marketing communications data	Until you unsubscribe.

On deletion we remove your account and content from active serving immediately and purge stored copies as they age out of our backup-rotation window, currently approximately 35 days. Records the law requires us to keep are retained for the periods in the table above, namely payment and tax records, the immutable administrative audit trail, and any data under legal hold. Identity tied to an unresolved copyright or DMCA matter is retained for the copyright-limitations window under our takedown process.

Legal-hold and active-incident exceptions: if a court order, an active fraud investigation, or an open security incident requires longer retention of specific records, we retain only what is necessary for the duration of the obligation, and then delete.

7. Your rights

Depending on your jurisdiction, and in particular under the GDPR, the UK GDPR and the UK Data Protection Act 2018, the Swiss Federal Act on Data Protection, and the CCPA as amended by the CPRA and other applicable US state privacy laws, you may have the right to:

- **Access** your Personal Data.
- **Rectify** inaccurate data.
- **Delete** your data, the "right to be forgotten", subject to the legal-hold exceptions in Section 6.
- **Restrict** or **object** to certain processing.
- **Portability**, meaning receiving your data in a machine-readable format.
- **Opt out** of the sale or sharing of Personal Data. We do not sell Personal Data and we do not share it for cross-context behavioral advertising, so there is no such activity to opt out of.
- **Lodge a complaint** with your local data-protection authority. In the EEA that is your supervisory authority, in the UK the Information Commissioner's Office, and in California the California Privacy Protection Agency.

To exercise any of these rights, email `privacy@extraspecial.co`. We respond **within one month for GDPR and UK GDPR** requests, extendable by two further months for complex or numerous requests and with notice to you, and **within 45 days for CCPA and CPRA** requests, extendable by a further 45 days and with notice to you.

Where we process Personal Data on a customer's behalf as a processor, we will direct your request to that customer and assist them in responding, as provided in our Data Processing Agreement with them.

EU and UK representatives. Where ExtraSpecial is required by applicable data-protection law to appoint a representative in the EEA or the United Kingdom, ExtraSpecial will maintain the required representative and make the representative's contact information available as required by law.

8. Children

The Service is not directed at children under 16. We do not knowingly collect Personal Data from anyone under 16. If you believe a child has provided us Personal Data, contact `privacy@extraspecial.co` and we will delete it.

9. Security

We employ administrative, technical, and physical safeguards designed to protect Personal Data. These include industry-standard encrypted transport protocols, currently TLS 1.2 or higher for externally accessible endpoints; industry-standard encryption at rest, currently including AES-256 and provider-managed key-management controls where applicable; least-privilege access control; federated, short-lived credentials and multi-factor authentication for privileged administrative access; logging and monitoring of administrative actions; automated security, dependency, secret, and configuration scanning on a regular risk-based cadence; and a documented incident-response process.

Breach notification. If we become aware of a Personal Data Breach affecting Personal Data for which we act as a processor, we notify the applicable customer without undue delay in accordance with our Data Processing Agreement. Where ExtraSpecial has an independent legal notification obligation, we provide notification as required by applicable law.

No system is perfectly secure. If you discover a vulnerability, please report it to `security@extraspecial.co` under the coordinated-disclosure process published at /.well-known/security.txt, for which we commit to a 24-hour acknowledgment.

10. Cookies

We use **strictly-necessary cookies** for session authentication and security, including CSRF tokens and anti-fraud heuristics. We do **not** set third-party advertising or tracking cookies. Where a cookie banner is shown, which is the case for EEA and UK visitors, you can configure preferences for any non-essential cookies. The only non-essential category today is product analytics, and its default is off.

11. California-specific disclosures (CCPA / CPRA)

For California residents:

- **Categories of personal information collected**: identifiers (name, email, IP address), commercial information (subscription history), internet and network activity (Service usage and access logs), and inferences derived from usage patterns, used for product improvement only.
- **Categories of sources**: directly from you; from your interactions with the Service; and from our payment processor, Stripe.
- **Business and commercial purposes**: providing the Service, processing payments, security, support, and legal compliance.
- **Categories of third parties**: the service providers and subprocessors identified in Section 4 and on our public Subprocessor and Infrastructure Vendor List.
- **Do we sell or share personal data?** No. We do not sell Personal Data and we do not share it for cross-context behavioral advertising.
- **Sensitive personal information**: we collect login credentials, and payment data is processed by Stripe. We do not use sensitive personal information to infer characteristics about you.
- **Retention**: see Section 6.

To exercise CCPA or CPRA rights, email `privacy@extraspecial.co`. You may also use an authorized agent.

12. Changes to this Policy

We may update this Privacy Policy from time to time. The current version is published at `https://hyperlinked.io/legal/privacy.pdf`. ExtraSpecial may publish a clearly identified successor location, and once identified that location is the canonical location.

Each published version carries the version identifier and effective date shown in the document header. Historical versions remain retrievable.

We will communicate material changes at least 30 days in advance by email and through an in-app banner.

13. Contact

- General privacy questions: `privacy@extraspecial.co`

- Security and vulnerability reports: `security@extraspecial.co`, per /.well-known/security.txt
- Legal questions: `legal@extraspecial.co`

The plain-language summary of this policy is our Customer Data Handling explainer, published at `https://hyperlinked.io/legal/data-handling.pdf`. Where the explainer and this Privacy Policy differ, this Privacy Policy governs.