



Privacy Policy

Estalytics Ltd trading as Stalytics

Last Updated: 2026/07/17

Document Version: 1.0

For an accessible HTML version of this document, visit:

<https://stalytics.com/privacy/privacy-policy.php>

1. Our Commitment to Your Privacy

- 1.1 This Privacy Policy outlines how Stalytics (“we”, “us”, “our”) collects, uses, and protects your personal data. Our commitment is to operate with transparency and integrity. We process personal data in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. This Privacy Policy explains how we collect and use your personal data. If you have any questions, please contact us.
- 1.2 Capitalised terms used in this Privacy Policy, including “Services”, “Service”, “Service Agreement”, “Statement of Work”, “Data Processing Agreement”, “Client” and “Deliverables”, have the meanings given to them in Stalytics’ [Master Terms & Conditions](#) where applicable, unless the context requires otherwise. Words in the singular include the plural and words in the plural include the singular.
- 1.3 “Website” means the website operated by Stalytics at <https://stalytics.com> and any related Stalytics webpage, subdomain, landing page or online form that links to this Privacy Policy.

2. Controller & Contact Information

- 2.1 For the purpose of the UK General Data Protection Regulation (UK GDPR), the data controller is Estalytics Ltd (Company No: 16412155), registered at 65 Lansdown Crescent, Bath, United Kingdom, BA2 0JX.
- 2.2 For any data protection enquiries, you can contact us at: privacy@stalytics.com
- 2.3 We are registered with the Information Commissioner’s Office (ICO) under registration number ZB950355.

Estalytics Ltd (trading as Stalytics)
Registered Office: 65 Lansdown Crescent, Bath, United Kingdom, BA2 0JX
Registered in England and Wales
Company No: 16412155 | VAT No: 494843934 | ICO Reg: ZB950355
Email: support@stalytics.com

3. The Information We Collect

- 3.1 We adhere to the principle of data minimisation, collecting only what is necessary to deliver our Services and improve your experience. We do not intend to collect special category data and ask that you do not submit such information unless strictly necessary.
- 3.1.1 Information You Provide Directly:
- 3.1.1.1 Your name, email address, telephone number and business contact details where provided.
 - 3.1.1.2 Details about your business, website, enquiry, Service request, project, compliance concern or audit/snapshot requirements.
 - 3.1.1.3 Website/page URLs, business information, supporting context, documents, files or materials that you choose to submit to us.
 - 3.1.1.4 Payment, billing, invoice, Service Agreement, clickwrap acceptance, quotation and order information where you purchase or request a Service.
 - 3.1.1.5 Any other personal data, business data or confidential information you choose to include in communications, forms, uploaded files or supporting materials.
- 3.1.2 Information We Collect Automatically:
- 3.1.2.1 IP address. IP addresses may be processed in server logs for security, fraud prevention, and system integrity purposes.
 - 3.1.2.2 Browser type, version, and device information.
 - 3.1.2.3 Pages visited, actions taken, and timestamps.
- 3.1.3 Our Use of Cookies:
- 3.1.3.1 We currently set only strictly necessary cookies and use cookieless analytics, so no consent is required. If we introduce non-essential cookies in future, we will obtain consent via a banner. See our [Cookie Policy](#).
- 3.1.4 Client Services, Evidence and Audit-Related Data:
- 3.1.4.1 When providing website compliance risk snapshots, website compliance risk audits or related Services, we may process information connected with the Client's website, submitted URLs, website pages, cookie and tracker behaviour, browser storage, network/script observations, consent mechanisms, policy materials, screenshots, evidence references, working notes, reports and Deliverables.
 - 3.1.4.2 Screenshots, evidence captures, browser storage records, network observations or uploaded files may incidentally contain personal data. We take reasonable steps to minimise, avoid, redact or limit unnecessary personal data where appropriate and practicable.
 - 3.1.4.3 Clients should not upload or submit unnecessary personal data, special category data, sensitive information, confidential third-party information or unrelated materials unless specifically requested or clearly required for the relevant Service.

- 3.1.4.4 For most enquiries, purchases, business communications, Service administration, billing, Website use and Client account handling, Stalytics acts as a Data Controller.
- 3.1.4.5 Stalytics may act as a Data Processor only where this is expressly required by the nature of the Service and set out in a Service Agreement, Statement of Work, [Data Processing Agreement](#) or written instruction agreed with the Client.
- 3.1.4.6 Where Stalytics acts as a Data Processor, the Client remains responsible for its own compliance obligations as Data Controller, including having an appropriate lawful basis, privacy information and authority to provide relevant personal data to Stalytics.
- 3.1.5 AI-Assisted Tools:
 - 3.1.5.1 We may use carefully selected AI-assisted tools to support drafting, analysis, quality control and document preparation.
 - 3.1.5.2 Where we use such tools, we aim to minimise unnecessary personal data and apply human review before relying on outputs in Deliverables provided to Clients.
 - 3.1.5.3 We do not use AI-assisted tools to make automated decisions about individuals that produce legal or similarly significant effects.

4. How We Use Your Data & Our Lawful Basis

- 4.1 In accordance with Article 6 UK GDPR, we only process personal data where a lawful basis applies. The purposes for which we process your data and the legal grounds for that processing are as follows:
 - 4.1.1 To provide our Services to you, including website compliance risk snapshots, website compliance risk audits, report preparation, evidence review, document preparation, Service administration, Client communication and delivery of agreed Deliverables: Contractual Necessity.
 - 4.1.2 To respond to enquiries submitted through the Website (including contact forms), provide requested information, and (where applicable) take steps at your request prior to entering into a contract (for example providing a quote): Legitimate Interests and/or Contractual Necessity (as applicable).
 - 4.1.3 For order fulfilment, payment handling, Service records and audit trail purposes, including transaction records, Service Agreement records, clickwrap acceptance records, quotation records, invoice records, delivery records and related internal records: Contractual Necessity, Legal Obligation and Legitimate Interests.
 - 4.1.4 To communicate with you regarding active projects, billing, and contractual matters: The lawful basis for this processing is Contractual Necessity.
 - 4.1.5 To understand aggregate Website use and performance, we use Cloudflare Web Analytics. Cloudflare states that its browser beacon does not store data in, or access storage data from, a visitor's device, including cookies, Local Storage, Session Storage or IndexedDB. It processes ephemeral performance information relating to the current webpage and does not create a persistent visitor identifier. We use this information only for aggregate Website usage and performance measurement and not for advertising, profiling or cross-site tracking. Our lawful basis under UK GDPR is Legitimate Interests. Further information is available in [Cloudflare's Privacy Policy](#).

- 4.1.6 For legal and tax compliance: We retain records as required by UK law. The lawful basis for this is Legal Obligation.
- 4.1.7 We may contact business clients or business contacts with Service-related communications: Contractual Necessity and/or Legitimate Interests. We will only send marketing communications where we have a lawful basis to do so and will provide an appropriate way to opt out where required.
- 4.1.8 Where we send marketing communications to existing business customers, we do so under the 'soft opt-in' rule under PECR, which permits us to market similar services to existing customers. You may opt out of marketing communications at any time by emailing privacy@stalytics.com. We do not send unsolicited direct marketing to individuals who are not existing customers without their prior consent.
- 4.1.9 We may use bot-protection and security technologies, such as Cloudflare Turnstile or equivalent tools, to help protect our forms, Website and systems from spam, abuse and automated misuse: Legitimate Interests.
- 4.1.10 To create, maintain and retain working files, reports, evidence records, screenshots, audit notes, quality-control records and Service delivery records where required to perform the Service, evidence work completed, manage disputes, maintain professional records and improve internal Service quality: Contractual Necessity and Legitimate Interests.
- 4.1.11 We do not carry out automated decision-making or profiling that produces legal or similarly significant effects.
- 4.2 Where we rely on Legitimate Interests as our lawful basis, we have carried out a balancing assessment to ensure that our interests do not override your fundamental rights and freedoms.
- 4.3 Our Promise: We will never sell, rent, or trade your personal data.

5. Who We Share Your Data With

- 5.1 Depending on the Service, these providers may act as our processors, independent controllers, or joint controllers for certain processing activities, as set out in their own privacy information and terms.
- 5.2 Where a provider processes personal data on our behalf as a processor, we put in place appropriate data protection terms (such as a data processing addendum where offered) and appropriate safeguards. In other cases, providers may process personal data as independent controllers under their own terms and privacy notices.
- 5.3 We only share personal data with trusted third-party providers where necessary to operate our business, provide our Website, deliver Services, process payments, manage records, communicate with Clients, prepare documents, secure our systems or comply with legal obligations.
 - 5.3.1 Stripe: We use Stripe to securely process payments, manage transactions and support payment-related records.
 - 5.3.2 IONOS: We use IONOS for the Website hosting, domain-related services, email hosting, email forwarding and secure file-sharing services including HiDrive.

- 5.3.3 Cloudflare: We use Cloudflare for Website security, content delivery, performance monitoring, Cloudflare Web Analytics and Cloudflare Turnstile. Cloudflare Web Analytics provides aggregate, cookieless Website usage and performance statistics. Cloudflare states that its browser beacon does not store or access browser storage data and does not create a persistent visitor identifier. Cloudflare Turnstile protects Website forms from spam, abuse and automated misuse. For Turnstile processing, Stalytics acts as the Data Controller and Cloudflare generally acts as our processor; Cloudflare may also act as an independent controller for the limited purposes described in its Turnstile Privacy Addendum. Cloudflare is based in the United States. Applicable international transfers are covered through the safeguards described in Cloudflare's Data Processing Addendum and privacy information. See [Cloudflare's Privacy Policy](#) and [Cloudflare's Turnstile Privacy Addendum](#).
- 5.3.4 Zoho: We may use Zoho services, including Zoho Sheets, for non-personal templates and operational materials only. We do not store Client personal data or populated Client audit records in Zoho.
- 5.3.5 Canva: We may use Canva to create and manage non-personal document templates and design assets only. We do not process Client personal data or Client deliverables in Canva.
- 5.3.6 AI-assisted tools. We use large-language-model providers to help draft, analyse, structure and quality-check audit workbooks, reports and related Deliverables. The providers we currently use are OpenAI (ChatGPT) and Anthropic (Claude), both based in the United States. We make best efforts to redact or minimise personal data before it is submitted, but limited information — typically the client's business name and the name of the website owner or contact — may be processed by these tools where necessary to produce the Deliverable. We apply human review before relying on any output. International transfers to these providers are covered in section 6, and they are listed in our sub-processor register.
- 5.3.7 Local systems and storage: We may store working files, evidence, reports, Service records and business records on local systems, local storage devices and internal business systems with appropriate access controls.
- 5.3.8 Legal, regulatory, professional or public authorities: We may disclose personal data where required by law, regulation, court order, legal process, professional obligation or where necessary to establish, exercise or defend legal rights.

6. International Data Transfers

- 6.1 Some of our service providers may process personal data outside the United Kingdom. Where international transfers occur, we rely on adequacy regulations where applicable, and/or appropriate safeguards such as the UK International Data Transfer Agreement (IDTA) and/or the UK Addendum to the EU Standard Contractual Clauses, as implemented by the relevant provider. You may request information about these safeguards by contacting us.

7. How We Protect Your Data

- 7.1 We employ appropriate technical and organisational security measures to protect personal data, including HTTPS encryption, secure hosting environments, restricted access controls, password protection, multi-factor authentication where supported by service providers, access limitation, local file controls, reasonable redaction/minimisation practices for evidence materials, and regular review of business systems where appropriate.

- 7.2 If a personal data breach occurs that is likely to result in a risk to your rights and freedoms, we will aim to notify the Information Commissioner's Office within 48 hours of becoming aware of it. In all cases, we will notify the ICO without undue delay and, where feasible, no later than 72 hours after becoming aware of the breach, as required by UK GDPR. Where the breach is likely to result in a high risk to your rights and freedoms, we will also notify you without undue delay.

8. Data Retention

- 8.1 We retain personal data only for as long as is reasonably necessary for the purposes for which it was collected, including Service delivery, contractual records, accounting, legal compliance, dispute handling, insurance, audit trail, quality control, security and business administration.
- 8.2 Enquiry records, incomplete enquiry records and abandoned checkout records may be retained for up to 24 months on the basis of Legitimate Interests (enquiry handling, fraud prevention, audit trail, Service improvement, dispute handling and business administration purposes) unless a longer period is required by law or a legitimate business need.
- 8.3 Client Service Agreements, clickwrap acceptance records, quotation records, invoices, payment records, delivery records and related contractual or financial records may be retained for up to 6 years where required, on the basis of Legal Obligation (tax/accounting record-keeping) and Legitimate Interests (dispute handling, audit trail).
- 8.4 Final reports, Deliverables, evidence packs, screenshots, working audit files, quality-control records and related Service records may be retained for up to 6 years where required, on the basis of Legitimate Interests (professional records, dispute and insurance defence) and, where applicable, Contractual Necessity.
- 8.5 Email correspondence and business communications may be retained for up to 6 years on the basis of Legitimate Interests (relationship and dispute management).
- 8.6 Analytics data: We use Cloudflare Web Analytics, which is cookieless and does not set cookies or track visitors across sites.
- 8.7 Security and server logs are retained for up to 30 days on the basis of Legitimate Interests (security and system integrity). This is for security monitoring, fraud prevention and system integrity purposes, unless a longer period is required to investigate suspected misuse, security incidents, fraud, technical issues or legal claims.
- 8.8 Backup copies may persist for a limited period according to the backup cycles of our systems and service providers before being overwritten or deleted in the ordinary course of business.
- 8.9 Where we no longer need personal data, we will delete, anonymise or securely archive it where appropriate.

9. Your Data Protection Rights

- 9.1 Under UK data protection law, you have rights including:

- 9.1.1 Your right of access: You have the right to ask us for copies of your personal information.
- 9.1.2 Your right to rectification: You have the right to ask us to rectify information you think is inaccurate.
- 9.1.3 Your right to erasure: You have the right to ask us to erase your personal information in certain circumstances.
- 9.1.4 Your right to restriction of processing: You have the right to ask us to restrict the processing of your information in certain circumstances.
- 9.1.5 Your right to object to processing: You have the right to object to the processing of your personal data in certain circumstances.
- 9.1.6 Your right to data portability: You have the right to ask that we transfer the information you gave us to another organisation, or to you, in certain circumstances.
- 9.1.7 Your right to withdraw consent: Where we are relying on your consent to process data, you may withdraw it at any time.
- 9.2 Where we rely on Legitimate Interests as our lawful basis, you have the right to object to that processing at any time. You also have an absolute right to object to the processing of your personal data for direct marketing purposes.
- 9.3 You are not required to pay any charge for exercising your rights. To make a request, please contact us at privacy@stalytics.com. We will respond within one month unless an extension is lawfully permitted under UK GDPR.
- 9.4 How to exercise rights:
 - 9.4.1 We may need to verify your identity before responding. We may ask for information to help us locate the data you are requesting. If a request is manifestly unfounded or excessive, we may refuse to act on it or charge a reasonable fee, as permitted by UK GDPR.
- 9.5 You also have the right to lodge a complaint with the Information Commissioner's Office at any time — see section 13.2 for details.

10. External Links & Third-Party Sites

- 10.1 Our Website may contain links to third-party websites, platforms or resources. We are not responsible for their privacy practices, cookie practices, security, content or terms. Please review their policies before sharing any personal data.

11. Children's Data

- 11.1 Our Services and Website are intended for business users and are not intended for children or for personal, household or non-business use. We do not knowingly collect personal data from anyone under 18. If you believe a child has provided us with personal data, contact us and we will take appropriate steps to delete it where required.

12. Changes to This Policy

- 12.1 We may update this Privacy Policy to reflect changes in our Services, data handling practices, service providers, technology, business operations or the law. The “Last Updated” date at the top of this policy will indicate the latest version.

13. Contact Us

- 13.1 For any questions, data requests, or concerns, please reach out:
- 13.1.1 Estalytics Ltd (trading as Stalytics);
 - 13.1.2 General support and enquiries: support@stalytics.com;
 - 13.1.3 Data protection enquiries: privacy@stalytics.com;
 - 13.1.4 Registered Office: 65 Lansdown Crescent, Bath, United Kingdom, BA2 0JX;
 - 13.1.5 Registered in England and Wales;
 - 13.1.6 Company No: 16412155;
 - 13.1.7 VAT No: 494843934;
 - 13.1.8 Information Commissioner’s Office registration number: ZB950355.
- 13.2 You also have the right to lodge a complaint with the UK’s data protection authority, the Information Commissioner’s Office (ICO). You can contact the ICO through its official website. We would appreciate the opportunity to address your concern first where appropriate.
- 13.3 If you have a data-protection complaint, contact privacy@stalytics.com. We will acknowledge it within 30 days and respond as soon as reasonably practicable. You may also complain to the ICO.