Data Processing Agreement

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/data-processing-agreement.php

Introduction

This Data Processing Agreement ("DPA") is entered into between the Client (the "Controller") and Estalytics Ltd trading as Stalytics (the "Processor").

This DPA applies only where, and to the extent that, Stalytics processes Personal Data on behalf of the Client as a Data Processor in the course of providing the Services. For most enquiries, purchases, billing, business communications and Client account handling, Stalytics acts as a Data Controller and this DPA does not apply; in those cases Stalytics' Privacy Policy applies. Stalytics acts as a Processor only where this is expressly required by the nature of the Service and set out in a Service Agreement, Statement of Work, written instruction, or this DPA, in accordance with clause 9 of the Master Terms & Conditions.

This DPA is incorporated into and forms an integral part of the Master Terms & Conditions (the "Principal Agreement") between the Parties. It takes effect on the effective date of the Principal Agreement and remains in force for so long as the Processor processes Personal Data on behalf of the Controller, or as otherwise agreed in writing.

Liability under this DPA: The liability, limitation and indemnity provisions of the Principal Agreement (Master Terms & Conditions) apply to claims arising under this DPA, subject to clause 10 (Liability) below.

1. Definitions

1.1 "Applicable Data Protection Law" means all laws and regulations applicable to the processing of Personal Data under the Principal Agreement, including the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

1.2 "Backups" means systems maintained by the Processor or its Sub-processors to store copies of Personal Data for disaster-recovery and business-continuity purposes.

1.3 "Controller" and "Processor" have the meanings given to them in Applicable Data Protection Law.

1.4 "Data Subject" means the identified or identifiable natural person to whom Personal Data relates.

1.5 "Data Subject Request" means a request made by a Data Subject to exercise any of their rights under Applicable Data Protection Law, including access, rectification, erasure, restriction, portability and objection.

1.6 "DPIA" or "Data Protection Impact Assessment" means an assessment of the impact of envisaged processing operations on the protection of Personal Data, as referred to in Applicable Data Protection Law.

1.7 "International Transfer Mechanism" means a lawful mechanism for transfers of Personal Data to a Third Country under Applicable Data Protection Law, including the UK International Data Transfer Agreement (IDTA), the UK Addendum to the EU Standard Contractual Clauses, reliance on UK adequacy regulations, or any other mechanism recognised under UK GDPR.

1.8 "Parties" means the Controller and the Processor, collectively.

1.9 "Personal Data" means any information relating to an identified or identifiable natural person that is processed by the Processor on behalf of the Controller as a result of the Services.

1.10 "Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

1.11 "Principal Agreement" means the Master Terms & Conditions entered into between the Parties, including any documents incorporated by reference such as this DPA.

1.12 "Processing", "processed" and "process" have the meanings given in Applicable Data Protection Law.

1.13 "Sub-processor" means any data processor engaged by the Processor to process Personal Data on behalf of the Controller.

1.14 "Supervisory Authority" means the Information Commissioner's Office (ICO) or any successor or other competent supervisory authority under Applicable Data Protection Law.

1.15 "Technical and Organisational Measures" means the security measures implemented by the Processor to ensure a level of security appropriate to the risk, as described in Section 3.

1.16 "Third Country" means any country or territory outside the United Kingdom to which Personal Data may be transferred.

1.17 Other capitalised terms used but not defined in this DPA have the meanings given in the Principal Agreement.

2. Processing of Personal Data

2.1 Roles of the Parties. For the purposes of Applicable Data Protection Law, in respect of the Personal Data processed under this DPA the Controller is the data controller and the Processor is the data processor.

2.2 Processor's obligations. The Processor shall process Personal Data only on the documented instructions of the Controller, including with regard to transfers to a Third Country, unless required to do otherwise by Applicable Data Protection Law (in which case the Processor shall, where legally permitted, inform the Controller of that legal requirement before processing). The Controller's instructions are deemed to include the processing necessary to provide the Services as set out in the Principal Agreement. The Processor shall promptly inform the Controller if, in its opinion, an instruction infringes Applicable Data Protection Law. The terms of the Principal Agreement and this DPA constitute the Controller's complete and final documented instructions for the processing of Personal Data; additional or different instructions require written agreement.

2.3 Details of processing:

2.3.1 Subject-matter: the processing of Personal Data contained within or connected to the Client's website, submitted URLs, forms, cookie and tracker behaviour, browser storage, network and script observations, consent mechanisms, policy materials, screenshots, evidence captures and related Client Materials, for the purpose of providing website compliance risk snapshots, website compliance risk audits and related Services as defined in the Principal Agreement.

2.3.2 Duration: for the period during which the Processor provides the relevant Services and processes Personal Data on the Controller's behalf, together with any retention period set out in the Privacy Policy or required by law, unless otherwise agreed in writing.

2.3.3 Nature and purpose: reviewing, capturing, analysing, summarising, structuring, quality-checking and reporting on Personal Data observed during the compliance review, in order to identify and describe compliance risks and to prepare the agreed Deliverables. The Processor does not host, develop, build or maintain the Controller's website, applications or systems as part of the standard Services.

2.3.4 Types of Personal Data: names, email addresses, telephone numbers, IP addresses, and other personal data that may incidentally appear within forms, screenshots, evidence captures, browser storage, network observations or other Client Materials reviewed during the Services. The Parties acknowledge that the Processor seeks to minimise and, where practicable, redact unnecessary Personal Data, but that limited Personal Data (for example, the business name and the name of a website owner or contact) may need to be processed to produce the Deliverables.

2.3.5 Categories of Data Subjects: the Controller's website visitors, enquirers, customers, contacts and, where relevant, personnel, whose Personal Data appears within the materials reviewed.

2.3.6 Special category and criminal offence data: the Services are not intended to involve the processing of special category data or criminal offence data. The Controller shall not provide such data to the Processor except where expressly requested by the Processor or clearly required for the agreed scope, and where the Controller has confirmed an appropriate condition for processing under Applicable Data Protection Law.

2.4 Assistance with DPIAs and prior consultation. The Processor shall provide the Controller with reasonable assistance with DPIAs and prior consultations with the Supervisory Authority, taking into account the nature of the processing and the information available to the Processor.

2.5 No legal advice. The Processor does not provide legal or regulatory advice, and nothing in this DPA or the Deliverables shall be construed as legal or regulatory advice to the Controller.

2.6 Statutory assistance and chargeable assistance:

2.6.1 The Processor will assist the Controller, at no additional charge, to the extent such assistance is reasonably required by Applicable Data Protection Law and is proportionate to the nature of the Services.

2.6.2 Where the Controller requires assistance that goes beyond the Processor's statutory obligations and reasonable support (for example, extensive forensic investigation at the Controller's request, or work outside normal support processes), such additional services may be treated as a Change Request under the Principal Agreement and charged only where agreed in writing in advance, including an estimate of fees.

2.7 Confidentiality. The Processor shall ensure that all persons authorised to process the Personal Data are bound by appropriate obligations of confidentiality.

2.8 Records of processing. The Processor shall maintain a record of the categories of processing activities carried out on behalf of the Controller, in accordance with Article 30(2) of the UK GDPR.

2.9 Controller warranties. The Controller warrants that it has a lawful basis for the processing of the Personal Data, that it is entitled to provide the Personal Data and the Client Materials to the Processor, and that it has provided all necessary notices and obtained all required consents under Applicable Data Protection Law.

2.10 For the avoidance of doubt, in the course of a Basic Website Compliance Risk Snapshot or Standard Website Compliance Risk Audit, Stalytics reviews publicly accessible website behaviour. Where personal data appears only incidentally within screenshots, browser storage, network observations or other evidence captured during such review, the Parties intend that Stalytics acts as a Data Processor in respect of that personal data and this DPA applies. Whether this DPA applies to a particular engagement is confirmed in the applicable Service Agreement, Statement of Work or written instruction.

3. Security Measures

3.1 The Processor shall implement and maintain appropriate Technical and Organisational Measures to ensure a level of security appropriate to the risk, taking into account the nature of the Services as a compliance-review and reporting service. These include, where applicable:

3.1.1 use of HTTPS/TLS encryption for the Processor's website, forms and secure file-sharing;

3.1.2 encryption of Personal Data at rest where appropriate (for example for stored evidence files or backups);

3.1.3 access controls, so that Personal Data is accessible only to authorised personnel and authorised Sub-processors on a need-to-know basis, subject to appropriate authentication;

3.1.4 confidentiality obligations for personnel and any contractors;

3.1.5 minimisation and, where practicable, redaction of unnecessary Personal Data within evidence, screenshots, working files and reports;

3.1.6 logging and monitoring of system access and data activity where supported by the relevant systems and providers;

3.1.7 backup and disaster-recovery procedures;

3.1.8 periodic review and testing of security measures;

3.1.9 an incident-response procedure for Personal Data Breaches, including notification to the Controller in accordance with Section 7.

3.2 The Controller acknowledges that some Technical and Organisational Measures depend on the features and configuration of third-party systems and Sub-processors used by the Processor.

4. Sub-processing

4.1 The Controller provides general written authorisation for the Processor to engage Sub-processors to perform parts of the Services. Current categories of Sub-processor include hosting, email and secure file-sharing providers, payment processors, document-preparation and spreadsheet tools, analytics and security tools, and AI-assisted (large-language-model) providers used to support drafting, analysis and quality control of Deliverables.

4.2 The Processor maintains a list of Sub-processors, including the service provided, location and processing purpose. This list will be provided to the Controller on request and may also be made available via a published Sub-processor list or schedule.

4.3 The Processor shall ensure that each Sub-processor is bound by written terms imposing data-protection obligations no less protective than those in this DPA, and the Processor remains liable to the Controller for the acts and omissions of its Sub-processors in relation to Personal Data, subject to Section 10.

4.4 The Processor shall notify the Controller in writing of any intended addition or replacement of a Sub-processor (including identity, country of processing and processing purpose) at least 14 calendar days before the change takes effect.

4.5 Controller right to object:

4.5.1 The Controller may object in writing, on reasonable data-protection grounds, to a new Sub-processor within 10 Business Days of the notice under clause 4.4.

4.5.2 If the Controller objects, the Parties shall use reasonable endeavours to agree an alternative. If no alternative can be agreed, either Party may terminate the Services materially affected by the proposed Sub-processor by written notice, without penalty, with the Controller's right to terminate limited to the Services materially affected.

4.6 AI-assisted tools. The Controller acknowledges that, as described in the Processor's Privacy Policy, the Processor uses large-language-model providers (currently OpenAI and Anthropic) to assist with drafting, analysis and quality control. The Processor applies data-minimisation and human review, and treats these providers as Sub-processors for the purposes of this DPA. The Controller's authorisation under clause 4.1 extends to these providers, subject to the notice and objection rights in clauses 4.4–4.5.

5. International Transfers

5.1 The Processor may transfer Personal Data to Sub-processors located outside the United Kingdom where necessary for the Services, provided that such transfers are subject to an appropriate International Transfer Mechanism in accordance with Applicable Data Protection Law.

5.2 Where required by Applicable Data Protection Law, the Processor shall ensure that an appropriate International Transfer Mechanism is in place and shall provide the Controller, on request, with reasonable information about the mechanism relied on for a given transfer.

6. Data Subject Rights

6.1 Taking into account the nature of the processing, the Processor shall provide reasonable assistance to enable the Controller to respond to Data Subject Requests, including requests relating to access, rectification, erasure, restriction, portability, objection and withdrawal of consent, within the timeframes required by Applicable Data Protection Law.

6.2 Where the Processor receives a Data Subject Request relating to Personal Data processed on behalf of the Controller, it shall promptly notify the Controller and shall not respond directly except on the Controller's documented instructions or as required by law.

6.3 Assistance that is clearly outside the scope of statutory compliance and the Processor's reasonable obligations may be treated as a Change Request under the Principal Agreement, charged in accordance with its rates, and only after written notice to the Controller including an estimate of fees.

7. Personal Data Breaches

7.1 The Processor shall notify the Controller without undue delay, and in any event within 48 hours, of becoming aware of a Personal Data Breach affecting Personal Data processed on behalf of the Controller.

7.2 The notification shall, to the extent available, include:

7.2.1 the nature and scope of the breach;

7.2.2 the categories and approximate number of Data Subjects affected;

7.2.3 the likely consequences of the breach;

7.2.4 the measures taken or proposed to address the breach and mitigate its effects; and

7.2.5 any Sub-processors involved and corrective actions taken.

7.3 The Processor shall provide reasonable assistance to the Controller in connection with the Controller's own breach-notification and communication obligations under Applicable Data Protection Law.

8. Data Deletion and Return

8.1 On termination or completion of the relevant Services, and at the Controller's written instruction, the Processor shall delete or return all Personal Data processed on behalf of the Controller, subject to clauses 8.2 to 8.5.

8.2 The Processor will use reasonable efforts to remove Personal Data from active systems promptly, and from backup media within a maximum of 90 calendar days of the Controller's deletion instruction, subject to the Processor's backup and retention cycles.

8.3 Where the Processor is required by law to retain some or all of the Personal Data, it shall notify the Controller in writing within 10 Business Days of the deletion instruction, specifying the legal basis and the estimated retention period, and shall retain the data only for as long as required.

8.4 The Controller acknowledges that Personal Data residing in Backups will not be immediately deleted but will be put beyond use and securely overwritten or decommissioned in the ordinary course in line with the Processor's standard backup and retention policies, and will not be restored or otherwise processed except where required by law.

8.5 Any return or deletion shall be carried out in accordance with Applicable Data Protection Law.

9. Audits and Information

9.1 The Processor shall, on reasonable prior written notice, make available to the Controller the information reasonably necessary to demonstrate compliance with Article 28 of the UK GDPR and this DPA.

9.2 As an alternative to an on-site audit, the Processor may, at its election, provide recent relevant independent third-party audit reports or certification evidence (for example SOC 2, ISO 27001, or a penetration-test summary, where available). Where such evidence reasonably addresses the Controller's audit objectives, any further on-site inspection may be limited to reasonable follow-up queries.

9.3 The Processor shall allow for and contribute to audits, including inspections, conducted by the Controller or an auditor mandated by the Controller, no more than once per year (save where required by a Supervisory Authority or following a Personal Data Breach).

9.4 Any audit must be proportionate, conducted during normal business hours, cause minimal disruption to the Processor's business, and be subject to the auditor being bound by appropriate confidentiality obligations. Audit findings containing Processor-confidential information shall be subject to confidentiality protections.

9.5 The Controller shall bear the reasonable costs of any audit it commissions, except where the audit reveals material non-compliance by the Processor with this DPA, in which case the Processor shall bear the reasonable incremental costs of that audit and shall promptly remedy any confirmed non-compliance.

10. Liability

10.1 The liability, limitation and indemnity provisions of the Principal Agreement, including clause 12 of the Master Terms & Conditions, apply to claims arising under this DPA except as expressly set out in this Section 10.

10.2 Nothing in this DPA or the Principal Agreement limits or excludes either Party's liability where such limitation or exclusion is not permitted by Applicable Data Protection Law, including liability to a Data Subject, liability for fraud or fraudulent misrepresentation, or liability for regulatory fines, penalties or enforcement action to the extent such liability cannot lawfully be limited or excluded.

10.3 For the purposes of this Section 10, "Data Protection Liability" means any liability, loss, claim, damage, fine, penalty, cost or expense arising out of or in connection with a Party's breach of this DPA or Applicable Data Protection Law in relation to Personal Data processed under or in connection with the Principal Agreement.

10.4 Subject to clause 10.2, each Party's aggregate liability to the other Party for Data Protection Liability shall not exceed:

10.4.1 for the Basic Website Compliance Risk Snapshot, the greater of ten times the total Fees paid or payable by the Client for that Service or £5,000;

10.4.2 for the Standard Website Compliance Risk Audit, the greater of five times the total Fees paid or payable by the Client for that Service or £15,000; and

10.4.3 for any Enterprise, bespoke, implementation, advisory or quote-based Service, five times the total Fees paid or payable by the Client for the relevant Service, unless a different data-protection liability cap is expressly stated in the applicable Proposal, Service Agreement, Statement of Work or other written agreement between the Parties. In agreeing any such different cap for higher-value, higher-risk or bespoke Services, the Parties may take into account the nature of the Services, the type and volume of Personal Data processed, the level of access granted, the use of any sub-processors, the allocation of responsibility between the Parties, and any relevant insurance position.

10.5 The liability cap in clause 10.4 applies instead of the general liability cap in clause 12.3 of the Master Terms & Conditions in respect of Data Protection Liability. It is not additional to, and shall not be aggregated with, the general liability cap except where expressly stated in the Principal Agreement.

10.6 A Party shall not be liable to the other Party under this Section 10 to the extent that the relevant liability, loss, claim, damage, fine, penalty, cost or expense was caused by the other Party's breach of this DPA, breach of the Principal Agreement, breach of Applicable Data Protection Law, negligence, wilful default, fraud, unlawful instruction, or failure to comply with its own data protection obligations.

10.7 Nothing in clause 10.4 limits or reduces any liability of a Party that is expressed to be uncapped under the Principal Agreement. In particular, where a liability arising under or in connection with this DPA also falls within clause 12.7B of the Master Terms & Conditions (Uncapped Client Liability) — including the Client's fraud, deliberate wrongdoing, breach of clause 18 (Anti-Bribery, Sanctions and Compliance), or unlawful use of the Services, Deliverables, Website or Stalytics materials — that liability shall be uncapped and the caps in clause 10.4 shall not apply to it.

11. Contact Point

11.1 The Processor's contact point for data-protection matters under this DPA is: privacy@stalytics.com.

12. Governing Law and Jurisdiction

12.1 This DPA is governed by and construed in accordance with the law of England and Wales, and the jurisdiction and dispute-resolution provisions of the Master Terms & Conditionsapply to any dispute arising out of or in connection with this DPA.

13. Contact Us

13.1 For any questions, data requests or concerns, please contact:

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.