Debiaser.ai Data Processing Agreement

Standard terms, version 1.0 — 7 July 2026.

Global Diversity Practice Limited. Company no. 06894073. Registered office: 37 Nab Lane, Shipley, BD18 4HQ, United Kingdom. VAT: GB 976147190. Data protection contact: data@globaldiversitypractice.com.

How this template is used

This is the standard Debiaser.ai Data Processing Agreement (version 1.0, dated 7 July 2026), published for procurement review. Organisation administrators can execute it electronically from the organisation page in the product: enter your organisation's particulars, review the completed agreement, sign, and Global Diversity Practice Limited countersigns. Both parties receive the executed copy for download.

This document is general information, not legal advice. Where a separately negotiated signed agreement conflicts with this template, the negotiated agreement controls.

About this agreement

This Data Processing Agreement (version 1.0, dated 7 July 2026) forms part of the agreement between the Customer and Global Diversity Practice Limited (“GDP”) for the Debiaser.ai service. It applies to GDP's processing of personal data contained in content the Customer submits to Debiaser.ai. Where a separately negotiated signed agreement conflicts with this DPA, the negotiated agreement controls. In respect of data-protection matters, this DPA prevails over the Debiaser.ai Terms of Service.

“UK GDPR”, “EU GDPR”, “controller”, “processor”, “personal data”, “data subject” and “personal data breach” have the meanings given in the UK GDPR and Data Protection Act 2018 and, where applicable, the EU GDPR.

1. Parties and roles

The parties are the customer organisation identified in the signature block or associated order (“Customer”), acting as controller, and Global Diversity Practice Limited, company no. 06894073, of 37 Nab Lane, Shipley, BD18 4HQ, United Kingdom, acting as processor when it processes personal data contained in workplace documents submitted to Debiaser.ai on the Customer's behalf.

Debiaser.ai reviews job descriptions, policies and workplace documents for unnecessary barriers and produces findings, explanations and revised wording for human review. GDP acts as an independent controller for Customer account, billing and service-security data, as described in the Debiaser.ai Privacy Policy.

2. Subject matter, duration, nature and purpose

Subject matter: hosting submitted documents, extracting text, routing appropriate model review, producing reports and revised documents, and operating accounts, credits, billing and security controls.

Duration: for the term of the Customer's use of the service. Review content is retained for the short service window described in the Privacy Policy — currently 7 days after review completion — unless deleted earlier by the user. Billing and ledger records may be retained where required for accounting, tax, fraud-prevention or legal obligations.

Purpose: to provide the Debiaser.ai service requested by the Customer, including document analysis, report generation, revised document generation, support, security and operational administration. GDP will not process Customer personal data for any other purpose.

3. Categories of data subjects and personal data

- Data subjects may include Customer users, document authors, candidates, employees, managers, workers, contractors or other people named in submitted workplace documents.
- Personal data may include names, business contact details, job titles, employment context, role requirements, qualifications, performance-related wording, accessibility-related text, policy text and other content the Customer chooses to submit.
- The Customer should avoid uploading unnecessary special-category data. If special-category data is included in a submitted document, processing is limited to the documented purpose of providing the service.

4. Processor obligations

GDP will, in respect of Customer personal data:

- process it only on the Customer's documented instructions (including the instructions constituted by the Customer's configuration and use of the service), unless required to do otherwise by law — in which case GDP will inform the Customer of that legal requirement before processing, unless the law prohibits doing so;
- immediately inform the Customer if, in GDP's opinion, an instruction infringes the UK GDPR or other applicable data-protection law;
- ensure that persons authorised to process the personal data are bound by appropriate obligations of confidentiality;
- implement and maintain the technical and organisational measures described in Annex B, reviewing and updating them as appropriate to the risk;
- assist the Customer, taking into account the nature of the processing, by appropriate technical and organisational measures, in responding to data subject rights requests under Chapter III of the UK/EU GDPR;
- assist the Customer in ensuring compliance with its obligations under Articles 32 to 36 (security, breach notification, DPIAs and prior consultation), taking into account the nature of the processing and the information available to GDP;
- delete or return personal data at the end of the services as set out in section 10;
- make available to the Customer all information necessary to demonstrate compliance with Article 28 UK/EU GDPR, and allow for and contribute to audits as set out in section 9.

5. Sub-processors

The Customer gives general written authorisation for GDP to engage the sub-processors listed in Annex C (also published at debiaser.ai/trust and in the Debiaser.ai subprocessor register). GDP imposes data-protection obligations on each sub-processor, by written contract, that are materially equivalent to those in this DPA, and remains fully liable to the Customer for the performance of each sub-processor's obligations.

GDP will give the Customer at least 30 days' advance notice of the addition or replacement of a sub-processor by updating the published register and emailing account holders with a signed DPA. The Customer may object within that notice period on reasonable, documented data-protection grounds. The parties will then work in good faith to resolve the objection; if it cannot be resolved, the Customer may terminate its use of the affected service and receive a pro-rata refund of unused purchased credits.

6. International transfers

Customer application data is hosted in the EU (AWS eu-west-1 via Convex). Transfers from the EEA to the UK are covered by the European Commission's adequacy decisions for the United Kingdom (renewed 19 December 2025, in force until 27 December 2031).

Where GDP or a sub-processor makes a restricted transfer of Customer personal data outside the UK or EEA (for example to the United States for AI analysis or transactional email), the transfer is protected by an appropriate safeguard: the EU Standard Contractual Clauses (Commission Decision 2021/914) together with

the UK International Data Transfer Addendum, the UK IDTA, or a UK/EU adequacy framework where applicable. The mechanism relied on for each sub-processor is set out in Annex C.

7. Security measures

- Passwordless one-time-code sign-in; no Debiaser.ai user passwords are stored.
- Authenticated server functions mediate all access to user and organisation content.
- Uploaded files, extracted text, model outputs, reports and revised documents have short retention deadlines enforced by automated purge jobs.
- Download URLs are short-lived and signed; public share links are opt-in, time-boxed and revocable.
- Provider-managed encryption protects traffic in transit and storage at rest.
- Rate limits protect authentication, trial claims, task creation, uploads and payments.
- Submitted content is treated as untrusted prompt data; the analysis model has no tools, database access or network access.
- Customer content is not used by Debiaser.ai to train AI models.

8. Personal data breach

GDP will notify the Customer without undue delay after becoming aware of a personal data breach affecting Customer personal data, and will provide the information reasonably available to GDP about the nature of the breach, the categories and approximate numbers of data subjects and records concerned, likely consequences, and the measures taken or proposed. GDP will cooperate with the Customer and take reasonable steps to mitigate the effects of the breach, and will assist the Customer with the Customer's own notification obligations under Articles 33 and 34.

9. Audit and information rights

GDP will make available to the Customer information reasonably necessary to demonstrate compliance with Article 28, including the published Trust and Security documentation, this DPA, the subprocessor register, and summaries of relevant third-party attestations held by GDP's infrastructure providers.

Where that information is insufficient to demonstrate compliance, GDP will allow for and contribute to audits, including inspections, conducted by the Customer or an independent auditor mandated by the Customer (not a competitor of GDP), no more than once in any 12-month period except following a personal data breach, on at least 30 days' written notice, during business hours, under reasonable confidentiality obligations, and in a manner that does not give access to other customers' data. Each party bears its own costs of an audit.

10. Deletion and return of data

Review content is deleted from active service storage automatically 7 days after a review completes, and users can delete a review or close an account at any time, which purges its content. At the end of the services, or on the Customer's written request, GDP will delete remaining Customer personal data from active service storage within 30 days and, on request, confirm deletion in writing — except where retention is required by law (for example billing and accounting records), in which case the data remains protected by this DPA and is deleted when the legal requirement ends. The Customer can retrieve reports, revised documents and exports at any time before deletion using the in-product download and export functions.

Residual copies in infrastructure-provider managed backups are deleted in the ordinary course of backup rotation under each provider's backup-retention controls, and remain protected by this DPA until deleted.

11. Data subject requests

If GDP receives a request from a data subject relating to Customer personal data, GDP will not respond substantively (except to direct the data subject to the Customer) and will promptly forward the request to the Customer. The in-product deletion and export controls are the primary mechanism through which GDP assists with data subject rights.

12. Customer responsibilities

- Provide lawful instructions and maintain a lawful basis for submitting workplace documents to Debiaser.ai.
- Avoid submitting personal data that is unnecessary for the review purpose.
- Review model-generated findings and revised wording with appropriate human judgement before use; Debiaser.ai provides professional guidance, not legal advice.
- Use organisation, invitation and sharing controls only for authorised personnel, and keep signatory and contact details in this DPA accurate.

13. Liability, precedence and governing law

This DPA is subject to the limitations and exclusions of liability in the Debiaser.ai Terms of Service, except that nothing limits either party's liability where liability cannot lawfully be limited. In respect of data-protection matters this DPA prevails over the Terms of Service. This DPA is governed by the laws of England and Wales and the courts of England and Wales have exclusive jurisdiction, on the same basis as the Terms of Service.

Annex A — processing details

Service: Debiaser.ai workplace-document bias review. Processing operations: upload, extraction, storage during the retention window, AI analysis through the sub-processors in Annex C, report generation, revised document generation, account access, billing records, service email and security monitoring.

Retention: active review content is automatically deleted 7 days after review completion; failed reviews and abandoned drafts are also assigned deletion deadlines. Billing metadata and ledger records are retained where required. Frequency: continuous, driven by Customer use of the service.

Annex B — technical and organisational measures

Measures include access control, least-privilege server functions, short-lived signed download URLs, encryption in transit, provider-managed encryption at rest, rate limiting, operational alerting, structured model-output validation, prompt-injection hardening, short retention deadlines with automated purge jobs and purge monitoring, error-diagnostic scrubbing (no personal data sent to diagnostics by default), and segregation of production credentials.

Annex C — sub-processors and transfer mechanisms

The following sub-processors are engaged as at the date of this DPA. The live register is published at debiaser.ai/trust. Restricted transfers rely on the mechanism listed for each sub-processor.

Provider / entity	Purpose	Processing location	Transfer mechanism and terms
Convex / Convex, Inc.	Backend, database and file storage	EU — AWS eu-west-1 (primary application data)	Application data is hosted in the EU. Provider data-processing terms incorporate the EU Standard Contractual Clauses (2021/914) with the UK Addendum for any residual transfer (for example US-based support access).
Anthropic / Anthropic, PBC	AI analysis of submitted document content	United States	Anthropic Data Processing Addendum incorporating the EU Standard Contractual Clauses (2021/914) and the UK Addendum. API inputs and outputs are not used to train models; Anthropic may retain API data for up to 30 days for trust-and-safety purposes.
Vercel / Vercel Inc.	Web application hosting and edge delivery	Global edge network; server functions pinned to London (lhr1)	Vercel Data Processing Agreement incorporating the EU Standard Contractual Clauses (2021/914) and the UK Addendum.
Stripe / Stripe Payments Europe, Ltd. and affiliates	Payments, tax calculation, invoices and receipts	Global payment infrastructure	Stripe Data Processing Agreement incorporating Standard Contractual Clauses and the UK Addendum. Stripe is the sole holder of card details and acts as an independent controller for certain payment, fraud-prevention and regulatory data under its own privacy terms.
Resend / Resend (resend.com)	Transactional email: sign-in codes, receipts and service notices	United States / global email delivery	Resend Data Processing Addendum incorporating the EU Standard Contractual Clauses (2021/914) and the UK Addendum. Resend delivers mail through Amazon Web Services (Amazon SES, EU region endpoints) as its infrastructure sub-provider.

Provider / entity	Purpose	Processing location	Transfer mechanism and terms
Cloudflare / Cloudflare, Inc.	Turnstile bot protection for trial-credit claims	Global security network	Cloudflare Data Processing Addendum incorporating the EU Standard Contractual Clauses (2021/914) and the UK Addendum. Turnstile processes a security token and connection metadata only.
Sentry / Functional Software, Inc. (Sentry)	Error and performance diagnostics for the application	United States	Sentry Data Processing Addendum incorporating the EU Standard Contractual Clauses (2021/914) and the UK Addendum. Sentry is configured not to send personal data by default (sendDefaultPii disabled); it receives technical error diagnostics, not submitted documents.

Signature

This agreement is executed electronically through Debiaser.ai. The customer signatory confirms they are authorised to sign on behalf of the customer organisation; the agreement takes effect when countersigned by Global Diversity Practice Limited. Executed copies carry both signature blocks and a unique reference.