Data Processing Agreement

UK GDPR controller-to-processor template

> **DRAFT TEMPLATE FOR LEGAL REVIEW. This document is general information, not legal advice. Complete every [square bracket] field and obtain advice from a qualified solicitor before signing or relying on it.**

This Data Processing Agreement (DPA) is made between HYBRID E-BUSINESS SOLUTIONS LTD trading as AI Architect and [CLIENT LEGAL NAME] and forms part of the B2B Services Agreement dated [DATE].

This template assumes the Client is Controller and the Supplier is Processor for the processing described in Schedule 1. If the parties' roles differ, this document must be revised before use.

1. Definitions and scope

Controller, Processor, Data Subject, Personal Data, Personal Data Breach, Processing and Supervisory Authority have the meanings in UK Data Protection Law.

UK Data Protection Law means the UK GDPR, Data Protection Act 2018 and applicable Privacy and Electronic Communications Regulations, as amended.

This DPA applies only where the Supplier processes Personal Data on behalf of the Client under an SOW. The Services Agreement otherwise remains in force.

2. Roles and instructions

The Client is Controller and the Supplier is Processor for the processing in Schedule 1. The Client is responsible for the lawfulness, fairness and transparency of its processing and instructions.

The Supplier will process Personal Data only on the Client's documented instructions, including the Services Agreement, SOW and written directions, unless UK law requires otherwise. Where legally permitted, the Supplier will inform the Client before required processing.

The Supplier will promptly inform the Client if, in its reasonable opinion, an instruction infringes UK Data Protection Law and may suspend that instruction while the parties resolve the issue.

3. Confidentiality and personnel

The Supplier will ensure that people authorised to process Personal Data are subject to appropriate confidentiality obligations and receive relevant data protection and security guidance.

Access will be limited to personnel who need it to provide, secure or support the Services.

4. Security

Taking account of the state of the art, implementation cost, processing context and risk, the Supplier will maintain appropriate technical and organisational measures. The agreed baseline is in Schedule 2.

The Client is responsible for configuring Client-controlled accounts, permissions, retention and security features and for making appropriate backups unless the SOW states otherwise.

5. Subprocessors

The Client gives general written authorisation for the Supplier to use the subprocessors in Schedule 3. The Supplier will impose materially equivalent data protection obligations on each subprocessor.

The Supplier will give at least [15] days' notice of a new or replacement material subprocessor where reasonably practical. The Client may object on reasonable data protection grounds. The parties will work in good faith on an alternative; if none is reasonably available, either party may terminate the affected processing without penalty beyond fees for Services already provided and committed costs.

The Supplier remains responsible for its subprocessors' performance of applicable data protection obligations.

6. International transfers

The Supplier will not transfer Personal Data outside the United Kingdom unless permitted by UK Data Protection Law and supported by an adequacy regulation or appropriate safeguards.

Where required, the parties incorporate the UK International Data Transfer Agreement or UK Addendum to the EU Standard Contractual Clauses. The relevant transfer mechanism and supplementary measures should be recorded in Schedule 3.

7. Data subject rights

Taking account of the nature of processing, the Supplier will provide reasonable assistance for the Client to respond to requests from Data Subjects. If the Supplier receives a request relating to Client Personal Data, it will forward it to the Client and will not respond except on the Client's instruction or as required by law.

Additional work beyond normal service operation may be charged at agreed rates where permitted by law.

8. Personal Data Breaches

The Supplier will notify the Client without undue delay after becoming aware of a confirmed Personal Data Breach affecting Client Personal Data.

The notice will provide available information about the nature of the breach, likely consequences, affected data and people, mitigation and a contact point. Information may be provided in phases as the investigation develops.

Notification does not constitute an admission of fault. The Client is responsible for notifications to regulators and Data Subjects unless the parties agree otherwise.

9. Assistance and compliance information

The Supplier will provide reasonable assistance with security, breach assessment, data protection impact assessments and regulatory consultation, taking account of the nature of processing and information available to it.

The Supplier will make available information reasonably necessary to demonstrate compliance with Article 28 UK GDPR.

10. Audits

The Client may request relevant independent reports, certifications and written responses before requesting an on-site audit. If those materials are insufficient, the Client may conduct one proportionate audit in any 12-month period on at least 20 Business Days' notice, or sooner following a material breach or regulator request.

Audits must protect other customers, confidentiality and security, take place during normal business hours and avoid unreasonable disruption. The Client bears its audit costs and the Supplier may charge reasonable assistance costs unless the audit identifies a material breach by the Supplier.

11. Return and deletion

At the end of the relevant Services, the Supplier will, at the Client's choice, return or delete Client Personal Data unless law requires retention. Routine backup copies may remain until overwritten under normal cycles and will remain protected and unavailable for ordinary use.

12. Liability, priority and term

The liability provisions and caps in the Services Agreement apply to this DPA unless expressly varied. If this DPA conflicts with the Services Agreement on processing Personal Data, this DPA prevails.

This DPA continues while the Supplier processes Client Personal Data. Clauses that by nature should survive continue after processing ends.

Schedule 1. Processing details

Subject matter and purpose: [Describe the service and why Personal Data is processed.]

Duration: [Term of SOW plus agreed return/deletion period.]

Nature and operations: [Collection, access, hosting, organisation, retrieval, analysis, transmission, support, deletion.]

Categories of Data Subjects: [Client staff, customers, suppliers, service users or other groups.]

Types of Personal Data: [Identity, contact, account, usage, content, special category or criminal offence data. State NONE where excluded.]

Special category or high-risk data restrictions: [DETAIL]. Processing locations: [DETAIL]. Client instructions and retention: [DETAIL].

Schedule 2. Technical and organisational measures

Governance: defined owners, confidentiality obligations, risk-based policies and incident process.

Access: least privilege, unique accounts, appropriate authentication and prompt access removal.

Data protection: encryption in transit; appropriate storage protection; secrets kept outside source code; controlled production access.

Development: change control, dependency management, review and testing proportionate to risk.

Operations: logging and monitoring appropriate to the service, backup and recovery responsibilities documented in the SOW, vulnerability handling and incident escalation.

Data lifecycle: collection minimisation, environment separation where applicable, retention instructions and secure deletion subject to backup cycles.

Project-specific additions or exceptions: [DETAIL].

Schedule 3. Approved subprocessors and transfers

Replit, Inc. | Application development, hosting and infrastructure | Data/location: [CONFIRM FOR PROJECT] | Transfer safeguard: [CONFIRM].

[DATABASE/HOSTING PROVIDER] | [PURPOSE] | [LOCATION] | [SAFEGUARD].

[AI MODEL PROVIDER] | [PURPOSE AND DATA SENT] | [LOCATION] | [SAFEGUARD].

[EMAIL/INTEGRATION PROVIDER] | [PURPOSE] | [LOCATION] | [SAFEGUARD].

The parties must complete this schedule for the actual architecture before processing production Personal Data.

Signatures

Signed for the Client as Controller: _____ Name: [NAME] Title: [TITLE] Date: [DATE]

Signed for the Supplier as Processor: _____ Name: [NAME] Title: [TITLE] Date: [DATE]