

RegNexus Books - Data Processing Agreement (UK)

Version: 1.0

Date: 10 September 2026

This Data Processing Agreement ("**DPA**") forms part of the agreement under which **RegNexus Limited**, company number 17280006, of 19 Lewis Crescent, Wellington, Telford, England, TF1 2FQ ("**RegNexus**", "**Processor**", "**we**") provides RegNexus Books to the customer identified in the applicable order, online acceptance record or other agreement ("**Customer**", "**Controller**").

This DPA applies where RegNexus Processes Customer Personal Data on behalf of Customer in connection with RegNexus Books.

1. Definitions and interpretation

Applicable Data Protection Law means the UK GDPR, the Data Protection Act 2018, the Data (Use and Access) Act 2025 to the extent it amends or supplements UK data-protection law, the Privacy and Electronic Communications Regulations where applicable, and any binding replacement or amendment in force from time to time.

Customer Data means data submitted to, stored in or otherwise processed through RegNexus Books by or for Customer.

Customer Personal Data means Personal Data contained in Customer Data that RegNexus Processes on behalf of Customer.

Data Subject, Personal Data, Personal Data Breach, Process/Processing, Controller and Processor have the meanings given by Applicable Data Protection Law.

Sub-processor means another Processor engaged by RegNexus to Process Customer Personal Data.

Restricted Transfer means a transfer of Personal Data from the United Kingdom for which Applicable Data Protection Law requires an adequacy route, appropriate safeguard or applicable exception.

If this DPA conflicts with mandatory UK data-protection law, that law prevails. If this DPA conflicts with the main service agreement on data-protection matters, this DPA prevails, except that an applicable UK IDTA or EU SCCs plus UK Addendum prevail to the extent required by their terms.

2. Roles and scope

2.1 Customer is Controller of Customer Personal Data and RegNexus is Processor, except to the extent Applicable Data Protection Law determines otherwise for a particular processing activity.

2.2 RegNexus is an independent Controller for Personal Data it processes for its own purposes, including account/security administration, its own billing relationship, legal compliance, service protection and other purposes described in the RegNexus Books Privacy Notice. That controller processing is outside this DPA.

2.3 If Customer is itself a Processor acting for another Controller, Customer appoints RegNexus as its Sub-processor and warrants that it has authority to do so and to give the instructions in this DPA.

3. Customer instructions

3.1 RegNexus shall Process Customer Personal Data only: (a) on Customer's documented instructions; or (b) where UK law requires RegNexus to Process otherwise, in which case RegNexus shall inform Customer of that legal requirement before Processing unless the law prohibits it.

3.2 Customer's instructions include the service configuration, features Customer enables, authorised user actions, API/integration instructions and other written instructions agreed by the parties.

3.3 RegNexus shall immediately inform Customer if, in its opinion, an instruction infringes Applicable Data Protection Law. RegNexus may suspend the affected processing while the parties clarify a disputed instruction where necessary to avoid unlawful processing.

3.4 RegNexus shall not sell Customer Personal Data or Process it for advertising, general model training or another independent commercial purpose unless Customer has expressly instructed that

processing and it is lawful.

4. Customer responsibilities

4.1 Customer is responsible for: (a) the lawfulness, fairness and transparency of its Processing; (b) establishing and documenting an Article 6 lawful basis and, where applicable, an Article 9 or Article 10 condition; (c) providing required privacy information to Data Subjects; (d) ensuring Customer has the right to provide Customer Personal Data to RegNexus; (e) the accuracy and relevance of Customer's instructions and Customer Data; (f) responding to Data Subject requests as Controller; and (g) completing any DPIA for Customer's use of the service where required, with RegNexus's assistance under clause 10.

4.2 Customer acknowledges that payroll or other Customer Data may contain highly personal, special-category or criminal-offence information. Customer must not instruct RegNexus to Process such data unless Customer has identified the applicable legal condition and the use is within the documented service.

5. Confidentiality

5.1 RegNexus shall ensure that persons authorised to Process Customer Personal Data are bound by confidentiality obligations or an appropriate statutory duty.

5.2 RegNexus shall limit access to persons and systems that require it for the authorised processing.

6. Security

6.1 RegNexus shall implement and maintain appropriate technical and organisational measures under Article 32, taking account of the state of the art, implementation costs, nature/scope/context/purpose of Processing and risks to individuals.

6.2 The measures include, as appropriate to the service and verified production implementation:

- encryption in transit;
- password hashing and protected MFA secrets;
- organisation/tenant access controls;
- role-based access controls and authority controls;
- audit and security logging;
- rate limiting and web security controls;
- backup/restore and resilience procedures;
- vulnerability/dependency management;
- incident-response procedures;
- procedures for testing and reviewing the effectiveness of security controls.

6.3 RegNexus may update the measures where this does not materially reduce the overall security of the service.

6.4 Security information made available to Customer is confidential and may be redacted where reasonably necessary to protect the service or another customer.

7. Sub-processors

7.1 Customer gives RegNexus **general written authorisation** to appoint the Sub-processors identified in the current RegNexus Books Sub-processor List.

7.2 RegNexus shall maintain a current public Sub-processor List and a mechanism for Customers to receive change notices.

7.3 RegNexus shall notify Customer before adding or replacing a Sub-processor that will Process Customer Personal Data. Where reasonably practicable, RegNexus will give at least 5 calendar days' advance notice. A shorter period may be used where necessary for security, law, vendor discontinuation or continuity, provided RegNexus gives as much advance notice as reasonably practicable and explains the reason.

7.4 Customer may object during the notice period on reasonable, documented data-protection

grounds. The parties shall work in good faith to resolve the objection. If no commercially reasonable alternative is available, Customer may terminate the materially affected part of the service without penalty for future use of that affected service, subject to any committed fees for unaffected services stated in the main agreement.

7.5 RegNexus shall enter into a written contract with each Sub-processor imposing data-protection obligations that provide an equivalent level of protection for the relevant Article 28 requirements.

7.6 RegNexus remains liable to Customer for a Sub-processor's performance of its data-protection obligations to the extent required by Applicable Data Protection Law.

8. International transfers

8.1 Customer instructs RegNexus to make Restricted Transfers only where necessary to provide an enabled service and only using a lawful transfer route.

8.2 Where a recipient and transfer are covered by UK adequacy regulations, RegNexus may rely on that adequacy route, including the UK Extension to the EU-US Data Privacy Framework where its requirements are met.

8.3 Where a Restricted Transfer is not covered by adequacy, RegNexus shall use an appropriate safeguard permitted by Applicable Data Protection Law, which may include: (a) the UK International Data Transfer Agreement; (b) the European Commission Standard Contractual Clauses together with the UK International Data Transfer Addendum; or (c) another appropriate safeguard recognised by Applicable Data Protection Law.

8.4 Where required, RegNexus shall complete and document the applicable UK data-protection-test/transfer risk assessment and supplementary measures before relying on the safeguard.

8.5 Where RegNexus is a Processor and a non-UK provider is its Sub-processor, the processor-to-processor/module-three terms shall apply where that is the legally appropriate module.

8.6 RegNexus shall make available, on reasonable request, information about the applicable transfer mechanism, subject to lawful redaction.

9. Personal Data Breaches

9.1 RegNexus shall notify Customer of a Personal Data Breach affecting Customer Personal Data **without undue delay and in any event within 24 hours after RegNexus becomes aware of it.**

9.2 The initial notice may be preliminary. As information becomes available, RegNexus shall provide, to the extent known: (a) the nature of the breach; (b) categories and approximate numbers of affected Data Subjects and records where reasonably ascertainable; (c) likely consequences; (d) measures taken or proposed to contain, investigate and mitigate the breach; (e) a contact point for further information.

9.3 RegNexus shall reasonably assist Customer with its Articles 33 and 34 obligations.

9.4 RegNexus shall not notify affected Data Subjects or a supervisory authority on Customer's behalf unless Customer instructs it or Applicable Data Protection Law requires RegNexus to do so in its own capacity.

9.5 Customer remains responsible for deciding whether and when it must notify the ICO or affected individuals as Controller.

10. Data Subject rights, DPIAs and regulatory assistance

10.1 Taking account of the nature of Processing, RegNexus shall use appropriate technical and organisational measures to assist Customer in responding to requests under Chapter III UK GDPR.

10.2 If RegNexus receives a request relating solely to Customer Personal Data, RegNexus shall not substantively respond on Customer's behalf unless authorised or legally required; it shall direct or forward the request to Customer where practicable.

10.3 Taking account of the nature of Processing and information available, RegNexus shall reasonably

assist Customer with:

- security obligations under Article 32;
- breach assessment/notification under Articles 33 and 34;
- DPIAs under Article 35; and
- prior consultation with the ICO under Article 36.

10.4 RegNexus may provide standard security, DPIA, transfer and architecture information to meet repeated assistance requests. Bespoke assistance materially beyond ordinary service support may be charged at agreed reasonable rates unless required because of RegNexus's breach.

11. AI-assisted processing

11.1 Where Customer enables an AI-assisted feature that sends Customer Personal Data to an AI Sub-processor, Customer instructs that processing for the purpose of the enabled feature.

11.2 RegNexus shall: (a) use Customer Personal Data only as needed for that feature; (b) configure business/API services so Customer Personal Data is not used for general model training unless Customer has expressly opted in and the processing is lawful; (c) maintain the AI provider as a disclosed Sub-processor where it Processes Customer Personal Data; (d) apply the relevant international-transfer protections; (e) not represent processing as “zero retention” unless the relevant production endpoint/configuration has been verified as such.

11.3 Current OpenAI business/API terms state that API inputs and outputs are not used for model training by default. Data retention is endpoint/configuration dependent and may be up to 30 days under standard API handling; eligible Zero Data Retention controls are available only for qualifying use cases.

11.4 Where technically available, optional AI features may be disabled or scoped by Customer. RegNexus shall accurately describe any feature that cannot be used without AI processing before Customer enables it.

12. Audit and information rights

12.1 RegNexus shall provide Customer with information reasonably necessary to demonstrate compliance with Article 28.

12.2 RegNexus may satisfy routine audit requests first through current security documentation, independent assurance reports (if any), completed questionnaires and other relevant evidence.

12.3 If that evidence is insufficient, Customer may conduct or appoint an independent auditor to conduct an audit of RegNexus's relevant Processing, subject to: (a) reasonable prior written notice; (b) normal business hours; (c) reasonable scope designed to minimise disruption and protect other customers' data/security; (d) confidentiality; (e) ordinarily no more than once in any 12-month period, unless a material Personal Data Breach, regulator request or credible evidence of material non-compliance justifies an additional audit.

12.4 Customer bears its audit costs unless the audit identifies material non-compliance by RegNexus, in which case RegNexus shall bear its reasonable internal remediation costs and the parties will address reasonable audit costs under the main agreement.

12.5 Nothing in this clause restricts an ICO audit or statutory investigative power.

13. Records and compliance

13.1 RegNexus shall maintain records of categories of Processing carried out for customers to the extent Article 30(2) applies.

13.2 RegNexus shall cooperate with the ICO as required by Applicable Data Protection Law.

13.3 RegNexus shall make available information reasonably necessary for Customer to demonstrate that it has engaged a Processor providing sufficient guarantees under Article 28.

14. Return and deletion

14.1 On termination/expiry, and at Customer's choice, RegNexus shall return or delete Customer Personal Data, unless UK law requires storage.

14.2 RegNexus may provide a reasonable export window and technical export method as specified in the service terms.

14.3 Data remaining temporarily in backups after deletion shall be: (a) put beyond ordinary business use; (b) protected by the same security obligations; and (c) deleted through the normal backup-expiry/destruction cycle.

14.4 RegNexus shall not use retained backup data for another purpose.

15. Liability

15.1 Liability arising under this DPA is subject to the exclusions and caps in the main agreement except to the extent a limitation is prohibited by Applicable Data Protection Law or other applicable law.

15.2 Nothing in this DPA limits or excludes: (a) any right of a Data Subject under Applicable Data Protection Law; (b) the powers of the ICO; (c) liability that cannot lawfully be limited or excluded.

15.3 Each party remains responsible for regulatory penalties imposed on it, subject only to any recovery that is lawful and expressly permitted under the main agreement.

15.4 Before customer launch, the parties' Terms/MSA should specify the general liability cap and any separate data-protection/confidentiality/security super-cap. This DPA deliberately does not invent a monetary cap without alignment to RegNexus's insurance and commercial terms.

16. Term and governing law

16.1 This DPA starts when Customer becomes bound by the service agreement and continues for as long as RegNexus Processes Customer Personal Data.

16.2 Clauses that by their nature survive termination, including confidentiality, deletion, liability and audit relating to prior Processing, continue as necessary.

16.3 Subject to mandatory transfer-clause provisions, this DPA is governed by the law of England and Wales and the courts of England and Wales have jurisdiction as stated in the main agreement.

Schedule 1 - Processing details

Subject matter

Provision, operation, security and support of RegNexus Books and enabled accounting, reporting, payroll, tax, banking, integration, Horizon, Frontier and Nexus functions to the extent Customer uses them.

Duration

For the term of the customer agreement plus the documented return/deletion/backup-expiry period.

Nature and purpose

Hosting, storage, organisation, retrieval, calculation, transmission, support, security, backup, audit, reporting, integration and other processing necessary to provide Customer's enabled features on Customer's instructions.

Categories of Data Subjects

May include:

- Customer's authorised users and personnel;
- employees, workers, directors and contractors;

- customers, suppliers and business contacts;
- shareholders, beneficial owners and other corporate stakeholders;
- accountants, advisers and agents;
- individuals whose data appears in invoices, bills, bank transactions, payroll, tax records, documents or other Customer Data.

Types of Personal Data

May include:

- names, contact and business details;
- user/access identifiers;
- financial transactions, bank-related records and accounting entries;
- invoices, bills, payment and commercial records;
- payroll information, salary, tax codes and National Insurance numbers;
- tax and filing information;
- employment/role information;
- document content uploaded by Customer;
- audit, device, IP and security logs connected with Customer use;
- data returned from Customer-authorised integrations.

Special-category / criminal-offence data

Not required for ordinary core accounting in all cases, but may be present in Customer-supplied payroll, expense, document or transaction records. Customer is responsible for establishing the applicable Article 9/10 and DPA 2018 conditions and for instructing RegNexus lawfully.

Frequency

Continuous or as initiated by Customer/users during the service term.

Schedule 2 - Technical and Organisational Measures summary

RegNexus maintains measures appropriate to the risk, including the verified production controls described in clause 6. The detailed internal security architecture and incident procedures may be provided under confidentiality where reasonably necessary for due diligence.

Controls include:

- access authentication and role-based authorisation;
 - tenant/organisation access boundaries;
 - secure transport encryption;
 - password hashing and protected MFA information;
 - audit/security event logging;
 - rate limiting and application security controls;
 - backups and documented recovery procedures;
 - incident-response procedures;
 - authority/approval controls for material financial actions where enabled;
 - change/dependency monitoring and controlled deployment practices;
 - periodic testing and review of relevant controls.
-

Schedule 3 - Sub-processors

The current list is maintained in the **RegNexus Books Sub-processor List** and forms part of this DPA by reference.

The current Sub-processor List identifies the service providers engaged by RegNexus for Customer

Personal Data, their functions, principal processing locations and applicable UK transfer position.

Schedule 4 - Restricted Transfers

For each Restricted Transfer RegNexus shall record:

- exporter and importer;
- roles (Controller/Processor/Sub-processor);
- data/categories/purpose;
- destination and onward transfers;
- adequacy or appropriate safeguard relied upon;
- applicable SCC module/UK Addendum or IDTA details;
- UK data-protection-test/transfer risk assessment;
- supplementary measures and review date.

Customer authorises such transfers only as provided in clauses 3, 7 and 8.