

Data Processing Agreement

Processor terms between the customer firm (as controller) and Jurion AI (as processor) for personal data processed within the Jurion AI platform.

Document ID	JUR-LEG-003
Version	1.0
Effective date	2026-01-01
Last updated	2026-07-09
Category	privacy
Publisher	Jurion AI, jurion.uk

Subject to legal review

This document is provided for information only and remains draft until reviewed by a qualified solicitor. It does not constitute legal advice.

Jurion AI

info@jurion.uk
<https://jurion.uk>

Contents

1. Scope	3
2. Controller and processor roles	4
3. Nature and purpose of processing	5
4. Processor obligations	6
5. Security measures	7
6. Subprocessors	8
7. International transfers	9
8. Audit rights	10
9. Breach notification	11
10. Data deletion	12
11. Term	13
12. Governing law	14
13. General provisions and commercial protections	15
<i>Revision history</i>	17

1. Scope

This Data Processing Agreement ("DPA") applies where Jurion AI Limited ("Processor") processes personal data on behalf of the customer firm ("Controller") in the course of providing the Jurion AI platform ("Service") under the Terms of Service.

In the event of conflict between this DPA and the Terms of Service in respect of the processing of personal data, this DPA prevails.

2. Controller and processor roles

The Controller determines the purposes and means of processing personal data through the Service. The Controller is responsible for the lawfulness of the personal data submitted to the Service and for issuing appropriate instructions to the Processor.

The Processor processes personal data only on the documented instructions of the Controller, as set out in the Terms of Service, in this DPA and in the configuration of the Service.

3. Nature and purpose of processing

Nature: hosting, storage, retrieval, analysis, generation of AI Output, transmission, monitoring for security and support, and deletion, as required to provide the Service.

Purpose: enabling the Controller and its Authorised Users to use the Service for legal practice management and related activities.

Duration: for the term of the Terms of Service and any post-termination period required for the return or deletion of personal data.

Categories of data subjects: Authorised Users of the Controller, clients of the Controller, opposing parties, witnesses, counterparties, counsel, court personnel and other individuals referenced in Customer Data.

Categories of personal data: identity, contact, professional, financial, matter-related, correspondence and any other categories submitted by the Controller to the Service.

4. Processor obligations

Processing only on documented instructions of the Controller, unless required to do so by law binding on the Processor, in which case the Processor will inform the Controller of that legal requirement to the extent legally permitted.

Ensuring that personnel authorised to process personal data are bound by appropriate confidentiality obligations.

Implementing and maintaining the technical and organisational measures described in the Jurion AI Security Overview.

Assisting the Controller, taking into account the nature of the processing and the information available, in complying with the Controller's obligations under applicable data protection law in respect of security, breach notification, data protection impact assessments and prior consultation.

Assisting the Controller in responding to requests from data subjects to exercise their rights.

5. Security measures

The Processor implements administrative, technical and organisational measures appropriate to the risk, including access control, authentication, encryption in transit and at rest for supported components, tenant isolation, activity logging and vulnerability management. Further detail is set out in the Jurion AI Security Overview.

6. Subprocessors

The Controller authorises the Processor to engage the subprocessors listed in the Jurion AI Subprocessor List.

The Processor will impose written data protection obligations on each subprocessor that are no less protective than those in this DPA.

The Processor will maintain the Subprocessor List and will notify the Controller of the intended addition or replacement of a subprocessor with reasonable prior notice. The Controller may object on reasonable data protection grounds. Where the parties cannot agree on a resolution the Controller may terminate the affected part of the Service.

7. International transfers

Where personal data is transferred outside the United Kingdom or the European Economic Area, the parties will rely on the UK International Data Transfer Agreement, the UK Addendum to the EU Standard Contractual Clauses, or the EU Standard Contractual Clauses as applicable, together with any supplementary measures required.

8. Audit rights

The Processor will make available to the Controller information reasonably necessary to demonstrate compliance with this DPA, including summary results of independent assessments where available.

The Controller may audit the Processor's compliance with this DPA once per year on reasonable prior written notice, during business hours and in a manner that does not unreasonably interfere with the Processor's operations or with other customers. The parties will agree on scope, timing and confidentiality arrangements in advance. Additional audits may be carried out where reasonably required following a personal data breach affecting the Controller's data.

9. Breach notification

The Processor will notify the Controller without undue delay after becoming aware of a personal data breach affecting the Controller's data.

The notification will include, to the extent then known, the nature of the breach, the categories and approximate number of data subjects and records concerned, the likely consequences, and the measures taken or proposed to address the breach and mitigate its effects. Further information will be provided as it becomes available.

10. Data deletion

On termination or expiry of the Terms of Service, the Processor will, at the choice of the Controller, delete or return all personal data processed on behalf of the Controller, and delete existing copies unless applicable law requires storage of the personal data.

Backups containing personal data will expire in accordance with the Processor's standard backup rotation, subject to continued application of the security measures in this DPA until expiry.

11. Term

This DPA is effective from the effective date of the Terms of Service and continues until the Terms of Service terminate, except for any obligations that expressly or by their nature survive termination.

12. Governing law

This DPA is governed by the laws of England and Wales and is subject to the exclusive jurisdiction of the courts of England and Wales, without prejudice to any mandatory jurisdiction rules for data protection matters.

13. General provisions and commercial protections

These general provisions apply to and form part of this document. Where a specific clause elsewhere in this document, in the Terms of Service or in the Data Processing Agreement addresses the same subject matter in greater detail, that more detailed clause prevails to the extent of any conflict.

13.1 AI limitations

Artificial intelligence features are assistive. Outputs are produced automatically and may contain errors, omissions, out-of-date information, inaccurate citations or content that is inappropriate for a specific matter. Jurion AI does not warrant that any AI output is accurate, complete, current or fit for any particular purpose and does not warrant that the Service is free from all errors or interruptions.

13.2 Human review requirement

Customer must ensure that a suitably qualified person reviews and approves any AI output before that output is relied on for legal advice, sent to a client, filed with a court or regulator, executed as a contract or used to make a decision that materially affects any person. Professional judgement of the reviewing individual remains authoritative.

13.3 Customer responsibility

Customer is responsible for its use of the Service, for the accuracy and lawfulness of the data it submits, for the actions of its authorised users and for compliance with applicable law and professional rules including where relevant the SRA Standards and Regulations. Customer must maintain appropriate matter management, supervision, conflict-checking and file-retention practices independently of the Service.

13.4 Acceptable use

Use of the Service is subject to the Jurion AI Acceptable Use Policy. Customer must not use the Service for unlawful purposes, to infringe the rights of any person, to attempt to circumvent the security of the Service, to submit content that is unlawful or that Customer does not have the right to submit, or in a way that materially degrades the Service for other customers.

13.5 Liability limits

Nothing in this document limits or excludes any liability that cannot be limited or excluded under applicable law, including liability for death or personal injury caused by negligence and for fraud. Subject to that, neither party is liable for indirect, incidental, consequential, special or exemplary damages, or for loss of profit, revenue, goodwill, anticipated savings, business opportunity or reputational loss, however arising.

Subject to the above, each party's total aggregate liability arising out of or in connection with this document in any twelve-month period will not exceed the fees paid by Customer to Jurion AI in that period. To the maximum extent permitted by law, the Service is provided "as is" and Jurion AI disclaims all warranties, whether express or implied, including any implied warranties of satisfactory quality, fitness for a particular purpose and non-infringement, other than those that cannot be excluded under applicable law.

13.6 Pilot status

Where the Service or a specific feature is provided on a pilot, beta, preview, evaluation or early-access basis, that Service or feature is provided "as is", may change or be withdrawn at any time and is not covered by the service-level commitments applicable to generally-available features. Pilot terms in the applicable order or the Pilot Programme Terms prevail over inconsistent provisions in this document.

13.7 Third-party services

The Service integrates with third-party services including cloud infrastructure, model providers, email providers, calendar providers and payment providers. Those third parties operate under their own terms and privacy notices. Jurion AI is not responsible for the availability, performance or acts and omissions

of third parties beyond its reasonable control, and Customer's use of any third-party service through the Service is subject to that third party's terms.

13.8 Data protection roles

Where Jurion AI processes personal data on behalf of Customer in connection with the Service, Customer is the controller and Jurion AI is the processor, and the Jurion AI Data Processing Agreement governs that processing. Where Jurion AI processes personal data as controller (for example account and billing data of authorised users and website analytics), the Jurion AI Privacy Policy governs that processing.

13.9 Service changes

Jurion AI may from time to time modify, add to or remove features of the Service in order to improve it, to reflect changes in third-party services, to reflect changes in law or regulatory guidance or to maintain security. Jurion AI will not make changes that materially reduce the overall functionality of the Service during a paid subscription term without giving reasonable prior notice.

13.10 Suspension rights

Jurion AI may suspend access to the Service or to specific authorised users, in whole or in part, where Jurion AI reasonably believes that continued access presents a security risk, that fees are materially overdue, that use of the Service is in material breach of this document or the Acceptable Use Policy, or that suspension is required by law or by a request from a competent authority. Where practicable Jurion AI will notify Customer before suspending access and will restore access as soon as the relevant circumstances have been resolved.

13.11 Security responsibilities

Jurion AI implements the technical and organisational security measures described in the Jurion AI Security Overview. Customer is responsible for configuring the Service in line with its own security requirements, for managing authorised user access including timely off-boarding, for enabling multi-factor authentication for its administrators, for protecting credentials and end-user devices, and for the security of any data that Customer chooses to export from the Service.

13.12 Draft status

This document remains draft and is subject to legal review until reviewed and approved by a qualified solicitor. It is provided for information only, does not constitute legal advice and should not be relied on as a final legal instrument until it has been so reviewed.

Revision history

Version	Date	Summary
1.0	2026-01-01	Initial published version.