Data Processing Agreement ("DPA")

This Data Processing Agreement is incorporated into and forms part of the agreement between the Customer and Simpson Associates governing Customer's access to and use of the RedactXpert application. Capitalised terms not defined in this DPA shall take the meaning given in the RedactXpert Terms of Service (**Terms of Service**).

1. Interpretation

1.1 The definitions and rules of interpretation in this Data Processing Agreement are as follows.

AI Outputs: means any data, content, results, recommendations, classifications, summaries, predictions, analyses or other materials generated or produced by AI Functionality as part of the Services in response to Customer inputs or data.

Customer: shall mean the customer of Simpson Associates as detailed in the Order Form.

Customer Personal Data: Personal Data submitted to or processed by or on behalf of Simpson Associates in connection with the provision of the Services under the Agreement, but excluding personal data processed by Simpson Associates in its capacity as an independent Data Controller

Data Controller, Data Processor, Personal Data, Data Subject and process/processing: shall have the meanings given to them in the Data Protection Laws**.**

Data Protection Laws mean:

(a) to the extent the UK GDPR applies, the law of the United Kingdom or of a part of the United Kingdom which relates to the protection of personal data.

(b) to the extent the EU GDPR applies, the law of the European Union or any member state of the European Union to which the Supplier is subject, which relates to the protection of personal data.

EU GDPR means the General Data Protection Regulation (*(EU) 2016/679*).

Simpson Associates means Simpson Associates Information Services Limited**.**

Special Category Data: has the meaning given in Article 9 UK GDPR (and Article 9 EU GDPR where applicable).

UK GDPR: has the meaning given to it in the Data Protection Act 2018.

2. Customer Data

2.1 Both Parties agree to comply with all applicable requirements of the Data Protection Laws and acknowledge that this Clause 2 is in addition to, and does not relieve, remove or replace, a party's obligations or rights under the Data Protection Laws.

2.2 For the purposes of applicable Data Protection Laws, the parties acknowledge that:

(a) the Customer acts as the Data Controller in respect of Customer Personal Data processed in connection with the Services as detailed in Schedule 1 Part A;

(b) Simpson Associates acts as Data Processor in respect of Customer Personal Data when processing it on behalf of the Customer in accordance with the Agreement and as detailed in Schedule 1 Part A;

(c) Schedule 1 describes the subject matter, duration, nature and purpose of the processing and the Personal Data categories and Data Subject types in respect of which Simpson Associates may process the Personal Data for the purpose of delivering the Services.

2.3 Notwithstanding clause 2.2 Simpson Associates shall act as an independent Controller in respect of Personal Data processed by it for the following purposes:

(a) account management, billing and contract administration;

(b) compliance with legal and regulatory obligations;

(c) security monitoring, fraud detection and prevention, and maintaining the integrity of the Services; and

(d) anonymisation and aggregation of data for service improvement, analytics, and development of the Services, provided that such data does not identify the Customer or any individual.

2.4 The Customer shall ensure that, in respect of all Personal Data submitted to the Services, it has established and can demonstrate: (a) a valid lawful basis under Article 6 UK GDPR; (b) where Special Category Data is processed, a condition for processing under Article 9 UK GDPR; and (c) where criminal offence data is processed, a condition for processing under Article 10 UK GDPR and Schedule 1 to the Data Protection Act 2018, together with any appropriate policy document required thereunder. The Customer is solely responsible for providing all required transparency notices to Data Subjects, including disclosures relating to AI Functionality where applicable.

2.5 Without prejudice to the generality of Clause 2.2, Simpson Associates shall, in relation to any Personal Data processed in connection with the performance of its obligations under the Agreement:

(a) process Customer Personal Data only on the documented instructions of the Customer including as set out in the Agreement, any applicable Order Forms, and Customer's use of the Services and documented configurations, settings, administrator controls and other instructions submitted through the Services, unless Simpson Associates is required to do otherwise by applicable law. Where Simpson Associates is required by applicable law to process Customer Personal Data other than in accordance with the Customer's instructions, it shall inform the Customer of that legal requirement before processing, unless the law prohibits such notification.

For the avoidance of doubt, the Customer's documented instructions include the use of any AI Functionality incorporated into the Services.

(b) implement and maintain appropriate technical and organisational measures, consistent with industry standards and proportionate to the risks presented by the processing, to protect Customer Personal Data against unauthorised or unlawful processing and against accidental loss, destruction or damage. Such measures shall include, where appropriate, encryption, pseudonymisation, access controls, resilience of systems, backup and recovery capabilities, and regular testing of security effectiveness. In respect of Special Category Data, Simpson Associates shall apply enhanced safeguards proportionate to the sensitivity of such data. The applicable technical and organisational measures are set out in Part B of Schedule 1.

(c) implement governance measures proportionate to AI risk in relation to the AI Functionality;

(d) ensure that all personnel who have access to and/or process Customer Personal Data are obliged to keep the Personal Data confidential;

(e) only transfer Personal Data outside the UK as required for delivery of the Services and where it has implemented appropriate safeguards in accordance with applicable Data Protection Laws;

(f) provide reasonable assistance to the Customer taking into account the nature of the processing and information available to it, to enable the Customer, at the Customer's cost, to respond to any request from a Data Subject and in ensuring compliance with its obligations under the Data Protection Laws with respect to security, breach notifications, impact assessments and consultations with supervisory authorities or regulators;

(g) notify the Customer without undue delay and in any event within 72 hours of becoming aware of a Personal Data breach involving Customer Personal Data. Notification shall include the information required under Article 33(3) UK GDPR; and

(h) permit the Customer to audit Simpson Associates compliance with Data Protection Laws no more than once per year upon 30 days' written notice, during normal business hours, and subject to confidentiality obligations. Simpson Associates may satisfy audit obligations by providing third-party certifications (e.g. ISO 27001) and security reports.

2.6 The Customer provides general authorisation for Simpson Associates to;

(a) appoint sub-processors to process the Customer Personal Data, provided that Simpson Associates;

(i) ensures that the terms on which it appoints such sub-processors comply with applicable Data Protection Laws, and are consistent with the obligations imposed on Simpson Associates in this Clause 2;

(ii) remains liable for the acts and omissions of its sub-processors to the extent Simpson Associates would itself be liable under this Agreement for such acts or omissions, subject to the limitations of liability set out in clause 7.1;

(iii) maintain an up-to-date list of sub-processors, which shall be made available to the Customer in the Trust Centre; and

(iv) shall notify the Customer in writing of any intended addition or replacement of a sub-processor, giving not less than 30 days' prior notice ("**Sub-Processor Notice Period**")

(b) (unless otherwise agreed in writing) transfer Customer Personal Data outside of the UK (and where applicable the EEA) as necessary for delivery of the Services, provided that Simpson Associates shall ensure that all such transfers are made in accordance with Data Protection Laws including the requirement that the protection provided to the Customer Personal Data is not materially lower than that under the Data Protection Laws. For these purposes, the Customer shall promptly comply with any reasonable request of Simpson Associates, including any request to enter into standard data protection clauses adopted by the EU Commission from time to time (where the EU GDPR applies to the transfer) or adopted by the UK Information Commissioner from time to time (where the UK GDPR applies to the transfer).

2.7 The Customer may object to a proposed new or replacement sub-processor during the Sub-Processor Notice Period by notifying Simpson Associates in writing, provided that such objection must be based on reasonable and substantiated grounds relating to data protection. If the Customer does not object within the Sub-Processor Notice Period, the Customer shall be deemed to have accepted the new or replacement sub-processor.

2.8 Where the Customer raises a valid objection in accordance with Clause 2.7, Simpson Associates shall, within a reasonable timeframe, explore whether it can offer the Customer a practical alternative that avoids or addresses the Customer's concern , for example, by adjusting the scope of the affected Services, proposing an alternative sub-processor, or implementing additional safeguards. Simpson Associates shall not, however, be required to take any steps that would be disproportionately costly, operationally impractical, or materially disruptive to its business or its provision of services to other customers.

2.9 If Simpson Associates is unable to provide a reasonable alternative within 30 days of receiving the Customer's objection, the Customer may, as its sole and exclusive remedy, terminate the Agreement by giving written notice, such termination to take effect no later than the date of engagement of the new sub-processor. Upon such termination:

(a) the Customer shall pay all fees accrued and any committed costs incurred by Simpson Associates up to and including the effective date of termination; and

(b) neither party shall have any further liability to the other arising solely from such termination.

2.10 For the purposes of paragraph 2.6 (b), the Customer shall promptly comply with any reasonable request of Simpson Associates that is necessary to ensure the lawful making of such transfers, including (where relevant):

(a) the execution of standard data protection clauses adopted, approved or recognised from time to time by:

(i) the UK Information Commissioner or the Secretary of State under UK GDPR; and/or

(ii) the European Commission under EU GDPR (where EU GDPR applies to the transfer);

(b) assisting Simpson Associates with any additional measures or transfer risk assessments required to comply with the applicable data protection test set out in Data Protection Laws; and

(c) acknowledging that Simpson Associates may adopt or replace transfer mechanisms where required to comply with changes in Data Protection Laws, provided that such mechanisms ensure a level of protection for Customer Personal Data that is not materially lower than that required under UK GDPR.

2.11 Where the Customer is a competent authority and processes Customer Personal Data for any of the law enforcement purposes within the meaning of Part 3 of the Data Protection Act 2018, the parties shall comply with the applicable requirements of Part 3 of the Data Protection Act 2018 (including section 59) in respect of that processing, and the obligations of Simpson Associates in this Clause 2 shall be read as extending to the equivalent requirements applicable to processors under Part 3 of the Data Protection Act 2018.

3. Complaints, data subject requests and third-party rights

3.1 Simpson Associates must, at no additional cost, assist the Customer in complying with:

(a) data subject rights under Data Protection Laws (including rights of access, rectification, erasure, portability, objection, restriction, and rights in relation to automated decision-making), noting that Simpson Associates obligation extends to conducting reasonable and proportionate searches of Personal Data held within the Service application when assisting with such requests; and

(b) any information, assessment or interview notices served on the Customer by the Information Commissioner under Data Protection Laws.

3.2 Simpson Associates must notify the Customer without undue delay, and in any event within 3 Business Days, upon becoming aware of:

(a) any request from a Data Subject to exercise their rights under Data Protection Laws; or

(b) any complaint, notice or communication from a regulator or third party relating to the processing of Personal Data or either party's compliance with Data Protection Laws.

3.3 Simpson Associates will cooperate fully with the Customer, at no additional cost, in responding to any notification under clause 3.2, including by providing such information as the Customer reasonably requires within the timescales necessary for the Customer to meet its obligations under the Data Protection Legislation (including any applicable time period and any pausing of that period under Article 12A of the UK GDPR).

4. Term & Termination

4.1 Any provision of this DPA that expressly or by implication should come into or continue in force on or after termination of the Agreement in order to protect the Personal Data will remain in full force and effect

4.2 If a change in Data Protection Laws prevents either party from fulfilling all or part of its Agreement obligations, the parties may agree to suspend the processing of the Personal Data until that processing complies with the new requirements. If the parties are unable to bring the Personal Data processing into compliance with Data Protection Laws within 30 days, either party may terminate the Agreement on not less than 14 days written notice to the other party.

5. Data Retention and Deletion

5.1 Simpson Associates shall retain Personal Data only for as long as is necessary for the purposes of the processing as set out in the Retention Schedule at Part C of Schedule 1 to this Agreement, and shall not process Personal Data in a manner incompatible with those purposes.

5.2 Upon expiry of the applicable retention period, or upon termination or expiry of this Agreement (whichever is earlier), Simpson Associates shall:

(a) securely delete all Personal Data processed under this Agreement using methods that render the data irrecoverable (including, where appropriate, cryptographic erasure, secure overwriting, or certified destruction of physical media);

(b) delete all copies of the Personal Data held in any live systems, backups, archives, and disaster recovery environments within 90 days of the deletion trigger date;

(c) provide the Customer with written certification of the deletion within 14 days of completion; and

(d) ensure that any sub-processor complies with equivalent deletion obligations within the same timeframes.

5.3 Clause 5.2 is subject to any retention expressly permitted under Part C of Schedule 1 (including audit logs) and any retention required by applicable law. Any Personal Data so retained shall remain subject to the confidentiality, security and other protections of this DPA and shall be securely deleted at the end of the applicable retention period.

6. Data Protection Impact Assessment

6.1 Given the nature of the data processed (including special category data, criminal offence data, and data relating to vulnerable individuals), the Customer acknowledges that a Data Protection Impact Assessment (DPIA) may be required prior to commencing processing. Simpson Associates shall provide reasonable assistance to the Customer in carrying out such assessments.

7. Liability

7.1 Subject to clause 7.2 Simpson Associates' aggregate liability arising out of or in connection with this DPA (whether in contract, tort, negligence, breach of statutory duty or otherwise) shall be subject to the limitations and exclusions of liability set out in clause 15 of the Terms of Service.

7.2 Nothing in this DPA or the Terms of Service shall limit or exclude either party's liability for:

(a) fraud or fraudulent misrepresentation;

(b) death or personal injury caused by its negligence; or

(c) any liability which cannot be limited or excluded by applicable law;

Schedule 1 Part A - Personal Data Processing Schedule

In this Schedule, reference to the Processor is to Simpson Associates and to the Controller is to the Customer. Capitalised terms shall be defined as per the definitions in this DPA or in the Agreement.

1. Subject Matter and Duration of Processing

The Processor provides a cloud-based (SaaS) redaction platform that enables the Controller to upload, process, and redact personal data contained within documents in formats including, but not limited to:

- PDF (.pdf)
- Microsoft Word (.docx, .docm, .doc)
- Microsoft Excel (.xlsx, .xls)
- Microsoft PowerPoint (.pptx, .ppt)
- Images (.png, .jpeg, .jpg, .tiff, .tif)
- Text Files (.rtf, .txt)
- Emails (.eml, .msg)

The processing will continue for the term of the Agreement including any renewal periods, unless terminated earlier in accordance with the terms of the Agreement.

2. Nature and Purpose of Processing

The Processor processes personal data solely on behalf of the Controller for the following purposes:

- Optical Character Recognition (OCR) and natural language processing using AI functionality to identify personal data for redaction within uploaded document content
- Temporary storage and secure handling of uploaded files during the redaction workflow
- Generation of redacted output files for download by the Controller
- Provision of audit logs and processing records to the Controller
- Technical support, system access and platform maintenance activities that may involve incidental access to personal data

3. Categories of Data Subjects

Given the nature of the redaction platform and its use by law enforcement agencies, legal professionals, and public bodies, the categories of data subjects whose personal data may be processed are extensive and include, but are not limited to:

Category	Description
Suspects and accused persons	Individuals who are the subject of criminal investigations or proceedings
Victims and complainants	Individuals who have reported crimes or are identified as victims in case files
Witnesses	Individuals who have provided statements or evidence in connection with investigations or legal proceedings

Officers and staff	Police officers, civilian staff, and other law enforcement personnel referenced in operational records
Legal professionals	Solicitors, barristers, judges, and other legal practitioners named in case materials
Members of the public	Any individuals incidentally identified in documents
Minors and vulnerable persons	Children, young persons, and vulnerable adults referenced in safeguarding, family, or criminal case files
Informants and covert sources	Individuals whose identities require protection for safety or operational reasons
Third parties	Family members, associates, employers, medical professionals, social workers, and any other individuals referenced in uploaded materials
Controller's authorised users	Individuals who hold user accounts on the platform (name, email, role, activity logs)

4. Types of Personal Data

The platform may process an exceptionally broad range of personal data types, as the content uploaded for redaction reflects the full scope of information encountered in policing and legal contexts. The types of personal data include, but are not limited to:

4.1 Standard Personal Data

- Full names, aliases, and former names
- Dates of birth, age, and gender
- Home addresses, correspondence addresses, and location data
- Telephone numbers, email addresses, and other contact details
- National Insurance numbers and other government-issued identifiers
- Passport numbers, driving licence numbers, and immigration status
- Vehicle registration numbers and DVLA records
- Employment details (employer, role, workplace)
- Education and qualification records
- Financial information (bank account details, benefit records, income details)
- IP addresses, device identifiers, and digital account information
- Photographs, CCTV stills, and body-worn video imagery
- Voice recordings and audio transcripts
- Custody records and detention information
- Bail and remand conditions

4.2 Special Category Data (Article 9 UK GDPR)

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data (including facial images, fingerprints, and DNA profiles)
- Physical and mental health data (medical records, injury reports, mental health assessments, substance misuse information)

- Data concerning sex life or sexual orientation

4.3 Criminal Offence Data (Part 3, Data Protection Act 2018)

- Criminal convictions, cautions, and reprimands
- Allegations and intelligence relating to criminal activity
- Police National Computer (PNC) records
- Arrest records and charge sheets
- Court orders, sentences, and probation records
- Risk assessments and offender management data
- Witness statements and interview transcripts
- Forensic evidence and crime scene data

4.4 Law Enforcement Data

- Intelligence reports and briefing documents
- Covert surveillance material (RIPA-authorised)
- Automatic Number Plate Recognition (ANPR) data
- Communications data and intercept material
- Disclosure material prepared under the Criminal Procedure and Investigations Act 1996 (CPIA)
- Multi-agency safeguarding records

5. Sub-Processors

The Processor shall maintain an up-to-date list of sub-processors and shall notify the Controller of any intended changes to that list, giving the Controller [30] days to object. The current list of approved sub-processors is set out in Annex A to this Schedule.

Schedule 1 Part B - Technical and Organisational Security Measures

The technical and organisational measures applicable to the Services are set out in Simpson Associates' Security Measures document, which is incorporated into and forms part of this Agreement. A current copy is available via the Simpson Associates Trust Centre and shall be provided to the Customer on request. Simpson Associates may update these measures from time to time provided that it shall not make any change that materially reduces the overall level of security of the Services during the term.

-

Schedule 1 Part C - Data Retention and Deletion

Data Type	Retention Period	Deletion Method
Uploaded source files	7 days after the redaction request is started, unless otherwise instructed	Secure automated deletion
Redacted output files	7 days after the redaction request is started by the Controller, unless otherwise instructed	Secure automated deletion
Platform audit logs	2 years from date of creation	Automated purge from logging infrastructure
Security audit logs	2 years from the date of creation	Manual deletion
User account data	Duration of the Agreement plus 30 days	Secure deletion upon account decommissioning
Temporary processing cache	Automatically purged within 24 hours of job completion	Automated cache invalidation and secure wipe
Application telemetry and logs	90 days	Automated deletion