



Data Processing and Filtering Service Definition



Document title	Data Processing and Filtering Service Definition		
Reference No.	IF-SER-014	Version	1.0
Author	Lisa Washer, Head of Cyber		
Reviewed by	Chris De Wit, Senior e-Discovery Analyst		
Issue date	28/01/2026		



Data Processing and Filtering Service Definition

Document Control

Version	Name	Comment	Date
0.1	Lisa Washer	Initial Draft	07/01/2026
0.2	Chris De Wit	Review and Amendments	28/01/2026
1.0	Lisa Washer	Final review and publish	28/01/2026

Correlation Chart

Clause	FSR Code of Practice v2	ISO/IEC 17025:2017	ILAC-G19 :06/2022	ISO 9001:2015	ISO/IEC 27001:2022
Review of Requests, Tenders and Contracts	16	7.1	4.1, 4.7	8	4.2



Data Processing and Filtering Service Definition

Contents

Document Control.....	2
Correlation Chart.....	2
Contents	3
1. Data Processing and Filtering Service	4
1.1 Service Overview	4
1.2 Service Objectives	4
2. Service Features	5
3. Service Benefits	6
4. Scope of Service	7
4.2 In-scope activities	7
4.3 Out-of-scope activities	7
4.4 Assumptions, Dependencies and Constraints	7
5. Service Delivery Model	9
5.1 Engagement Model	9
5.2 Delivery Phases	9
5.3 Reporting and Deliverables	9
6. Exit and Offboarding	10
7. Roles and Responsibilities	11
7.1 Service Provider Responsibilities	11
7.2 Client Responsibilities.....	11
7.3 Legal, Compliance, and Investigation Stakeholders (Where Applicable).....	11
7.4 Joint Responsibilities.....	12



Data Processing and Filtering Service Definition

1. Data Processing and Filtering Service

1.1 Service Overview

- 1.1.1 The Data Processing and Filtering Service provides structured, defensible processing and reduction of electronically stored information (ESI) using established e-discovery workflows. The service enables organisations to efficiently prepare large and complex datasets for review, investigation, disclosure, or regulatory response by applying consistent processing, filtering, and quality control techniques.
- 1.1.2 The service is designed to reduce data volumes, improve relevance, and support accurate downstream review while maintaining transparency, auditability, and evidential integrity.

1.2 Service Objectives

- 1.2.1 The objectives of the Data Processing and Filtering Service are to:
- a) Reduce data volumes in a defensible and proportionate manner
 - b) Prepare datasets for efficient review and analysis
 - c) Apply consistent, repeatable filtering methodologies
 - d) Support compliance with legal, regulatory, and disclosure obligations
 - e) Provide clear audit trails and quality assurance



Data Processing and Filtering Service Definition

2. Service Features

2.1.1 Key features of the service include:

- a) **Defensible Processing Workflows** – Aligned to recognised e-discovery best practice
- b) **Scalable Data Reduction** – Suitable for large and complex datasets
- c) **Custom Filtering Criteria** – Tailored to matter-specific requirements
- d) **Metadata-Driven Analysis** – Accurate extraction and use of key metadata
- e) **Quality Assurance Controls** – Sampling and validation to support defensibility



Data Processing and Filtering Service Definition

3. Service Benefits

3.1.1 The service delivers the following benefits:

- a) Significant reduction in review volumes and cost
- b) Improved relevance and focus of review datasets
- c) Transparent and auditable processing decisions
- d) Reduced risk of over- or under-disclosure
- e) Faster progression to review or production stages



Data Processing and Filtering Service Definition

4. Scope of Service

- 4.1.1 The service is delivered using defensible e-discovery methodologies suitable for litigation, regulatory enquiries, internal investigations, and audits. Outputs are produced with transparency to support legal scrutiny and regulatory review. Engagements may be coordinated through legal counsel where privileged handling is required.

4.2 In-scope activities

- 4.2.1 The Data Processing and Filtering Service includes the following activities:

- a) Engagement scoping and processing strategy development
- b) Ingestion of ESI from agreed data sources
- c) De-duplication and near-duplicate identification
- d) File type normalisation and metadata extraction
- e) Date range, custodian, and keyword filtering
- f) Identification of system, non-user, or irrelevant data
- g) Application of inclusion and exclusion criteria
- h) Sampling and validation of filtered datasets
- i) Preparation of review-ready data outputs

4.3 Out-of-scope activities

- 4.3.1 Unless agreed separately, the following are out of scope:

- a) Legal advice or interpretation of disclosure obligations
- b) Substantive document review or coding services
- c) Ongoing continuous monitoring or data management
- d) Data collection without lawful authority

4.4 Assumptions, Dependencies and Constraints

- 4.4.1 Delivery of the Data Processing and Filtering Service is based on the following assumptions:

- a) The client has lawful authority and a valid legal basis to process all in-scope data, including any personal, sensitive, or regulated information.
- b) Data provided for processing is complete, accurate, and representative of the agreed scope.



Data Processing and Filtering Service Definition

- c) Processing criteria, including custodians, date ranges, keywords, and inclusion or exclusion rules, are clearly defined and approved prior to processing.
- d) The client will provide timely access to data, documentation, and relevant stakeholders to support delivery.
- e) Any legal privilege, confidentiality, or sensitivity considerations are identified by the client at the outset or as they arise.

4.4.2 Service delivery is dependent on the following factors:

- a) Availability and timely provision of agreed datasets in supported formats.
- b) Cooperation from third parties, system owners, or service providers where data resides outside direct client control.
- c) Stability of scope and filtering criteria; material changes may require reprocessing or impact timelines.
- d) Performance and capacity of underlying e-discovery platforms and secure processing environments.
- e) Input and decisions from client legal, compliance, or investigation teams to validate processing outcomes.

4.4.3 The following constraints may impact scope, timelines, or outcomes:

- a) Data quality issues, such as corruption, incomplete metadata, or inconsistent formats, may limit processing accuracy.
- b) Encryption, password protection, or proprietary file formats may restrict access or require additional effort.
- c) Forensic and e-discovery best practice prioritises defensibility and accuracy over speed, which may affect turnaround times.
- d) Statutory deadlines, court directions, or regulatory requirements may constrain processing approaches.
- e) Findings represent a point-in-time assessment based on the data provided and processing criteria applied.
- f) Service delivery is subject to specialist resource availability and agreed commercial terms.



Data Processing and Filtering Service Definition

5. Service Delivery Model

5.1 Engagement Model

- 5.1.1 The service is delivered on an ad-hoc or project basis and tailored to the specific matter. Scope, processing parameters, timelines, and deliverables are agreed at the outset.
- 5.1.2 The service is primarily delivered remotely using secure e-discovery platforms. On-site or hybrid delivery may be provided where required for access to restricted environments.
- 5.1.3 All data is handled using secure processing environments, access controls, and confidentiality safeguards. Data is processed solely for the agreed purpose and retained only for the agreed duration.

5.2 Delivery Phases

- 5.2.1 Delivery typically includes:
 - a) Scoping and processing strategy definition
 - b) Data ingestion and initial processing
 - c) Filtering and data reduction
 - d) Validation and quality assurance
 - e) Delivery of review-ready datasets
 - f) Engagement closure
 - g) Phases may be iterative to refine criteria and optimise results.

5.3 Reporting and Deliverables

- 5.3.1 Deliverables may include:
 - a) Processing and filtering logs
 - b) Data volume reduction metrics
 - c) Filter criteria documentation
 - d) Quality assurance and sampling summaries
 - e) Review-ready datasets



Data Processing and Filtering Service Definition

6. Exit and Offboarding

- 6.1.1 Upon completion, data is securely returned, retained, or destroyed in accordance with agreed instructions and applicable legal obligations. Access is revoked and engagement closure confirmed.



Data Processing and Filtering Service Definition

7. Roles and Responsibilities

7.1 Service Provider Responsibilities

- 7.1.1 The service provider is responsible for delivering the Data Processing and Filtering Service in accordance with the agreed scope, processing strategy, and recognised e-discovery best practice. This includes advising on appropriate processing and filtering methodologies, configuring processing parameters, and executing defensible ingestion, de-duplication, normalisation, and metadata extraction workflows.
- 7.1.2 The service provider will apply agreed filtering criteria, including date ranges, custodians, keywords, and exclusion rules, and will document all processing decisions and actions to maintain full auditability. Quality assurance activities, including sampling and validation of filtered datasets, will be performed to support defensibility and accuracy. The service provider is responsible for secure handling of data throughout the engagement, maintaining access controls, confidentiality safeguards, and chain-of-custody records where applicable. Regular status updates will be provided, and any risks, data quality issues, or scope changes will be escalated promptly.

7.2 Client Responsibilities

- 7.2.1 The client is responsible for confirming the lawful authority and legal basis to process all in-scope data and for defining the objectives, scope, and filtering criteria of the engagement. This includes identifying relevant custodians, systems, date ranges, and relevance parameters, and providing timely access to data and supporting documentation.
- 7.2.2 The client retains responsibility for legal interpretation, relevance determinations, privilege decisions, and disclosure obligations. The client will review and approve processing strategies, filtering outcomes, and deliverables as required and will provide timely decisions to avoid delays. The client is also responsible for communications with courts, regulators, or other third parties, where applicable.

7.3 Legal, Compliance, and Investigation Stakeholders (Where Applicable)

- 7.3.1 Where legal counsel, compliance teams, or investigation leads are involved, these stakeholders are responsible for advising on legal and regulatory requirements, approving filtering strategies, and overseeing handling of privileged, confidential, or sensitive data. They may review outputs, advise on escalation thresholds, and ensure alignment with litigation, regulatory, or investigative objectives. Coordination with the service provider supports legally defensible processing and filtering.



Data Processing and Filtering Service Definition

7.4 Joint Responsibilities

- 7.4.1 The service provider and client share responsibility for effective communication, timely decision-making, and escalation of issues that may impact scope, timelines, or compliance. Both parties are responsible for maintaining confidentiality, supporting transparency and auditability, and ensuring that service outputs are used appropriately and in line with agreed objectives.

*****END OF DOCUMENT*****