PII Detection Service Definition

Document title	PII Detection Service Definition		
Reference No.	IF-SER-026	**Version**	1.0
Author	Lisa Washer, Head of Cyber		
Reviewed by	Chris De Wit, Senior e-Discovery Analyst		
Issue date	28/01/2026		

PII Detection 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

PII Detection Service Definition

Contents

PII Detection Service Definition

1. PII Detection Service

1.1 Service Overview

1.1.1 The PII Detection Service provides structured identification and analysis of personally identifiable information (PII) and personal data across electronically stored information (ESI) using e-discovery techniques and workflows. The service supports organisations in understanding where personal data resides, how it is distributed, and the associated risk exposure across systems, repositories, and datasets.

1.1.2 Using defensible e-discovery processing, search, and analytics capabilities, the service enables accurate detection, classification, and reporting of personal data to support compliance, risk management, investigations, and regulatory readiness.

1.2 Service Objectives

1.2.1 The objectives of the PII Detection Service are to:

a) Identify and map personal data across large, complex datasets

b) Support compliance with data protection and privacy obligations

c) Reduce regulatory, legal, and operational risk

d) Enable defensible, repeatable personal data discovery

e) Provide actionable insight into data handling practices

2. Service Features

2.1.1 Key features of the PII Detection Service include:

a) **E-Discovery-Based Detection** – Proven methodologies for large-scale data analysis

b) **Multi-Source Coverage** – Email, documents, collaboration platforms, and file shares

c) **Configurable PII Models** – Customisable PII definitions aligned to regulations

d) **Defensible Workflows** – Repeatable, auditable detection processes

e) **Privacy-Aware Handling** – Controlled access to sensitive data

3. Service Benefits

3.1.1 The service delivers the following benefits:

a) Clear visibility of personal data locations and volumes

b) Improved compliance readiness and risk awareness

c) Reduced cost and effort of manual data discovery

d) Defensible evidence for audits and regulatory enquiries

e) Better-informed data governance decisions

4. Scope of Service

4.1.1 The service supports compliance with data protection frameworks such as UK GDPR, EU GDPR, and related privacy legislation. Outputs are produced using defensible e-discovery methods suitable for audit, investigation, or regulatory scrutiny. Engagements may be coordinated through legal counsel where privileged handling is required.

4.2 In-scope activities

4.2.1 The PII Detection Service includes the following activities:

a) Scoping and definition of PII categories and risk priorities

b) Identification of custodians, systems, and data repositories

c) Collection or ingestion of ESI using e-discovery workflows

d) Processing and indexing of data for analysis

e) Detection of PII using keyword searches, pattern matching, and analytics

f) Classification of PII types (e.g. identifiers, financial, health)

g) Sampling and validation of detection results

h) Reporting and visualisation of PII findings

4.3 Out-of-scope activities

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

a) Provision of legal advice or regulatory interpretation

b) Ongoing continuous monitoring services

c) Automated deletion or remediation of identified data

d) Investigation of systems without lawful authority

4.4 Assumptions, Dependencies and Constraints

4.4.1 Service delivery assumes lawful authority to process in-scope data, timely access to systems, and agreed PII definitions.

4.4.2 Constraints may include data quality, encryption, proprietary formats, third-party dependencies, and statutory or contractual limitations.

5. Service Delivery Model

5.1 Engagement Model

5.1.1 The service is delivered on an ad-hoc consultancy basis or as part of a defined project. Scope, data sources, 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 local systems or restricted environments.

5.1.3 All data is handled using secure environments, strict access controls, and confidentiality safeguards. Processing is limited to the agreed purpose and retention period.

5.2 Delivery Phases

5.2.1 Delivery typically includes:

a) Scoping and PII definition

b) Data ingestion and processing

c) PII detection and classification

d) Validation and quality assurance

e) Reporting and risk analysis

f) Engagement closure

5.2.2 Phases may be delivered sequentially or in parallel depending on dataset size and urgency.

5.3 Reporting and Deliverables

5.3.1 Deliverables may include:

a) PII detection summary reports

b) Breakdown of PII types and locations

c) Risk-based analysis and prioritisation

d) Audit-ready documentation of methods and results

e) Recommendations for remediation or further action

6. Exit and Offboarding

6.1.1 Upon completion, data is securely returned, retained, or destroyed in accordance with agreed instructions and applicable data protection obligations.

7. Roles and Responsibilities

7.1 Service Provider Responsibilities

7.1.1 The service provider is responsible for delivering the PII Detection Service in accordance with agreed scope, applicable data protection legislation, and recognised e-discovery best practice. This includes supporting scoping activities to define PII categories, risk priorities, and data sources; configuring detection criteria, search logic, and analytics; and executing defensible data ingestion, processing, and analysis workflows.

7.1.2 The service provider will manage secure handling of all in-scope data, applying appropriate access controls and confidentiality safeguards throughout delivery. The provider is responsible for validating detection results through sampling and quality assurance, maintaining clear audit trails of methods and decisions, and producing accurate, transparent reporting of findings. The provider will proactively identify delivery risks, data quality issues, or scope changes and escalate these in a timely manner.

7.2 Client Responsibilities

7.2.1 The client is responsible for confirming the lawful basis and authority to process personal data, including approval of PII definitions, scope, and intended use of outputs. The client will identify relevant custodians, systems, and repositories and facilitate timely access to data, documentation, and subject-matter experts.

7.2.2 The client retains responsibility for interpreting findings in a legal and regulatory context, determining remediation actions, and making decisions regarding data retention, deletion, or disclosure. The client is also responsible for communications with regulators, data subjects, or other third parties, and for ensuring internal governance and oversight throughout the engagement.

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

7.3.1 Where privacy officers, Data Protection Officers (DPOs), or legal counsel are involved, they are responsible for advising on regulatory interpretation, risk tolerance, and handling of sensitive or special category data. These stakeholders may review detection outputs, advise on escalation thresholds, and oversee privileged handling where required. Coordination with the service provider ensures that detection activities remain aligned with organisational policies and regulatory obligations.

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 defensible and

transparent processes, and ensuring that the service outputs are used appropriately and in line with agreed objectives.

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