Data Breach Analysis Service Definition

Document title	Data Breach Analysis Service Definition		
Reference No.	IF-SER-013	**Version**	1.0
Author	Lisa Washer, Head of Cyber		
Reviewed by	Chris De Wit, Senior e-Discovery Analyst		
Issue date	28/01/2026		

Data Breach Analysis Service Definition

Document Control

Version	Name	Comment	Date
0.1	Lisa Washer	Draft Template	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 Breach Analysis Service Definition

Contents

1. Data Breach Analysis Service

1.1 Service Overview

1.1.1 The Data Breach Analysis Service provides structured, evidence-based analysis to determine what data has been accessed, disclosed, altered, or exfiltrated during a data breach or suspected security incident. The service focuses on identifying affected data types, data subjects, and systems to support regulatory assessment, notification obligations, legal response, and remediation activities.

1.1.2 Using forensic and e-discovery methodologies, the service enables organisations to establish the scope, sensitivity, and potential impact of compromised data in a defensible and auditable manner.

1.2 Service Objectives

1.2.1 The objectives of the Data Breach Analysis Service are to:

a) Identify data impacted by a confirmed or suspected breach

b) Determine categories and sensitivity of compromised data

c) Establish affected data subjects and records

d) Support regulatory risk assessments and notification decisions

e) Provide defensible evidence for audit, legal, and regulatory scrutiny

2. Service Features

2.1.1 Key features of the service include:

a) **Data-Centric Breach Analysis** – Focused on identifying compromised data

b) **Forensic and e-Discovery Methods** – Defensible analysis of large datasets

c) **Sensitive Data Classification** – Identification of regulated and high-risk data

d) **Audit-Ready Outputs** – Transparent documentation of methods and findings

e) **Regulatory Alignment** – Outputs aligned to GDPR and breach reporting needs

3. Service Benefits

3.1.1 The service delivers the following benefits:

a) Clear understanding of breach scope and affected data

b) Improved confidence in regulatory notification decisions

c) Reduced risk of under- or over-reporting

d) Defensible evidence for regulators and courts

e) Faster progression to remediation and recovery

4. Scope of Service

4.1.1 The service supports compliance with data protection legislation, including UK GDPR and EU GDPR breach assessment requirements. Engagements may be coordinated through external legal counsel to support legally privileged handling. Outputs are designed to support regulatory enquiries, audits, and litigation.

4.2 In-scope activities

4.2.1 The Data Breach Analysis Service includes the following activities:

a) Incident scoping and breach context review

b) Identification of affected systems, accounts, and data repositories

c) Forensic and logical analysis of accessed or exposed data

d) Review of logs, artefacts, and access records to determine data exposure

e) Classification of data types (e.g. personal, special category, financial)

f) Estimation of volume and number of affected records or data subjects

g) Assessment of data accessibility, encryption, and protection measures

h) Advisory support for regulatory and legal decision-making

i) Reporting of findings and limitations

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) Live containment, remediation, or system recovery

c) Negotiation or communications with threat actors

d) Continuous monitoring or managed response services

4.4 Assumptions, Dependencies and Constraints

4.4.1 Delivery of the Data Breach Analysis Service is based on the following assumptions:

a) The client has lawful authority and a valid legal basis to access, analyse, and process all affected systems, logs, and data repositories.

b) Accurate and timely information is provided regarding the nature, timing, and suspected scope of the breach.

c) Relevant systems, accounts, and data sources remain available for analysis and have not been materially altered prior to examination, except where required for containment.

d) Logging, audit trails, and data retention practices were enabled and operational at the time of the incident.

e) The client will provide timely access to subject-matter experts, system owners, and documentation to support interpretation of findings.

f) Any legal privilege, confidentiality, or sensitivity considerations are identified and communicated promptly.

4.4.2 Service delivery is dependent on the following factors:

a) Availability, completeness, and accuracy of logs, access records, and system artefacts necessary to determine data exposure.

b) Timely access to affected systems, cloud platforms, third-party services, or backups where relevant data resides.

c) Cooperation from third-party service providers or suppliers where data or logs are externally hosted.

d) Timely decision-making and input from client legal, privacy, and security stakeholders, particularly where regulatory deadlines apply.

e) Stability of scope; significant changes to incident understanding may require additional analysis and affect timelines.

4.4.3 The following constraints may impact the scope, timelines, or certainty of findings:

a) Incomplete, overwritten, or unavailable logs may limit the ability to definitively determine data access or exfiltration.

b) Encryption, anonymisation, or tokenisation may reduce the risk of data compromise but may also limit visibility into accessed content.

c) Technical limitations of systems, proprietary platforms, or third-party environments may restrict analysis depth.

d) Findings represent a point-in-time assessment based on available evidence and may not capture all historical activity.

e) Forensic and evidential best practice prioritises accuracy and defensibility over speed, which may affect delivery timelines.

f) Service delivery is subject to specialist resource availability and agreed commercial terms.

5. Service Delivery Model

5.1 Engagement Model

5.1.1 The service is delivered on an ad-hoc consultancy basis following a confirmed or suspected breach. Scope, timelines, and deliverables are agreed at initiation.

5.1.2 Services are primarily delivered remotely using secure analysis environments. On-site or hybrid delivery may be provided where required.

5.1.3 All data is handled using secure systems, controlled access, and confidentiality safeguards. Processing is limited to the agreed purpose and retained only for the agreed duration.

5.2 Delivery Phases

5.2.1 Delivery typically includes:

a) Incident scoping and data impact definition

b) Data source identification and access

c) Forensic and logical data analysis

d) Data classification and impact assessment

e) Validation and quality assurance

f) Reporting and advisory support

5.2.2 Phases may overlap depending on urgency and regulatory timelines.

5.3 Reporting and Deliverables

5.3.1 Deliverables may include:

a) Data impact assessment reports

b) Breakdown of affected data categories and volumes

c) Identification of affected data subjects

d) Methodology and limitation statements

e) Regulatory-ready summary outputs

6. Exit and Offboarding

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

7. Roles and Responsibilities

7.1 Service Provider Responsibilities

7.1.1 The service provider is responsible for delivering the Data Breach Analysis Service in accordance with the agreed scope, applicable data protection legislation, and recognised forensic and e-discovery best practice. This includes supporting breach scoping to understand the incident context, identifying affected systems and data repositories, and conducting structured analysis to determine what data has been accessed, disclosed, altered, or exfiltrated.

7.1.2 The service provider will perform forensic and logical analysis of logs, artefacts, and datasets to identify affected data types, volumes, and data subjects. The provider is responsible for classifying data by sensitivity, assessing protective measures such as encryption or access controls, and documenting assumptions, limitations, and confidence levels associated with findings. Secure handling of all in-scope data will be maintained throughout the engagement, with clear audit trails, validation checks, and quality assurance activities. The service provider will produce evidence-based reports and provide advisory support to assist informed regulatory and legal decision-making, promptly escalating material risks or uncertainties.

7.2 Client Responsibilities

7.2.1 The client is responsible for confirming lawful authority and legal basis to access and analyse affected systems and data. This includes providing accurate incident context, identifying relevant systems, accounts, and data sources, and facilitating timely access to logs, repositories, and subject-matter experts.

7.2.2 The client retains responsibility for regulatory notifications, communications with supervisory authorities, affected individuals, and other stakeholders, and for determining legal and compliance actions arising from the findings. The client is also responsible for reviewing and approving outputs where required and for ensuring internal governance, decision-making, and record-keeping obligations are met.

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

7.3.1 Where Data Protection Officers (DPOs), privacy teams, legal counsel, or security leads are involved, these stakeholders are responsible for interpreting findings in the context of regulatory thresholds, legal risk, and organisational policy. They may advise on notification obligations, risk severity, and mitigation actions, and may coordinate legally privileged handling of outputs. These stakeholders also support alignment between technical findings and regulatory or legal responses.

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 affect breach assessment accuracy, regulatory timelines, or compliance outcomes. All parties are responsible for maintaining confidentiality, supporting transparency and auditability, and ensuring the analysis is conducted proportionately, defensibly, and in line with applicable legal and regulatory requirements.

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