Data Subject Access Request (DSAR) Service Definition

Document title	Data Subject Access Request (DSAR) Service Definition		
Reference No.	IF-SER-015	**Version**	1.0
Author	Lisa Washer, Head of Cyber		
Reviewed by	Chris De Wit, Senior e-Discovery Analyst		
Issue date	28/01/2026		

Data Subject Access Request (DSAR) 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 Subject Access Request (DSAR) Service Definition

Contents

1. Data Subject Access Request (DSAR)

1.1 Service Overview

1.1.1 The Data Subject Access Request (DSAR) Service provides structured, defensible support to organisations responding to requests from individuals exercising their data protection rights under applicable data protection legislation, including the UK GDPR and Data Protection Act 2018.

1.1.2 The service supports the identification, review, and disclosure of personal data held across systems, devices, and repositories, ensuring responses are accurate, timely, and compliant while minimising operational disruption and regulatory risk.

1.2 Service Objectives

1.2.1 The objectives of the DSAR Service are to:

a) Enable compliant and timely DSAR responses

b) Reduce regulatory and litigation risk

c) Support accurate identification of personal data

d) Ensure lawful handling of third-party and exempt data

e) Provide defensible audit trails and reporting

2. Service Features

2.1.1 Key features of the DSAR Service include:

a) **Structured DSAR Workflow** – Repeatable, defensible end-to-end process

b) **Cross-System Data Identification** – Coverage across systems, devices, and repositories

c) **Privacy-Aware Review** – Controlled handling of third-party and exempt data

d) **Secure Data Handling** – Compliant processing and storage of personal data

e) **Audit-Ready Outputs** – Clear documentation of decisions and actions

3. Service Benefits

3.1.1 The DSAR Service delivers the following benefits:

a) Improved regulatory compliance and confidence

b) Reduced risk of incomplete or inaccurate disclosures

c) Reduced internal resource burden

d) Clear audit trail for regulators and courts

e) Consistent, repeatable DSAR handling

4. Scope of Service

4.1 In-scope activities

4.1.1 The DSAR Service includes the following activities:

a) Initial DSAR scoping and validation

b) Identification of relevant data sources and custodians

c) Collection and processing of personal data

d) Review and filtering of data for relevance

e) Identification and handling of exemptions and third-party data

f) Redaction and preparation of disclosure datasets

g) Support for extensions, clarifications, and correspondence

h) Production of compliant response packages

4.2 Out-of-scope activities

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

a) Provision of legal advice or representation

b) Management of ongoing subject correspondence

c) Continuous DSAR monitoring services

d) Investigation of data beyond agreed scope

4.3 Assumptions, Dependencies and Constraints

4.3.1 Delivery of the DSAR Service is based on the following assumptions:

a) The client is the lawful data controller or has appropriate authority to process the DSAR.

b) DSAR requests have been received and validated by the client in accordance with applicable data protection legislation.

c) The scope of the DSAR, relevant time periods, data subjects, and systems are clearly defined and agreed.

d) The client provides timely access to in-scope systems, data repositories, and custodians.

e) Appropriate internal approvals and governance processes are in place to support data identification, review, and disclosure.

4.3.2 Service delivery is dependent on:

a) Availability, accuracy, and completeness of data held across client systems and third-party platforms.

b) Cooperation from internal stakeholders, including IT, HR, Legal, and Compliance teams.

c) Timely clarification of scope changes, exemptions, or redaction requirements.

d) Reliance on third-party providers or cloud platforms where data is externally hosted.

e) Client decisions regarding legal privilege, exemptions, or refusal grounds where applicable.

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

a) Data retention limits, prior deletion, or system limitations may result in incomplete datasets.

b) Encryption, proprietary formats, or legacy systems may restrict access or increase processing effort.

c) DSAR timelines are governed by statutory deadlines, which may constrain processing approaches.

d) Findings represent a point-in-time assessment based on data available during processing.

e) Best practice prioritises accuracy, defensibility, and data protection compliance over speed.

f) Service delivery is subject to specialist availability, technical feasibility, and agreed commercial terms.

5. Service Delivery Model

5.1.1 The DSAR Service is delivered through a structured, phased approach designed to ensure compliance, accuracy, and defensibility while minimising operational impact. Engagements are initiated on an ad-hoc basis following receipt of a Data Subject Access Request, with scope, data sources, timelines, and deliverables agreed at the outset.

5.1.2 Delivery typically follows defined phases, including request intake and validation, data source identification, data collection and processing, review and redaction, disclosure preparation, and engagement closure. Phases may be delivered sequentially or in parallel, depending on complexity and statutory response deadlines:

a) **Request Intake and Validation** - Receipt and validation of the DSAR, including identity verification, scope clarification, and response timeframe confirmation.

b) **Data Source Identification -** Identification of relevant systems, devices, data repositories, and custodians likely to contain personal data.

c) **Data Collection and Processing -** Collection and secure processing of in-scope data in preparation for review.

d) **Review and Redaction -** Review of data for relevance, application of exemptions, third-party protection, and redaction where required.

e) **Disclosure Preparation -** Preparation of disclosure packages and supporting documentation.

f) **Response Support and Closure -** Support for response delivery, record retention, and engagement closure.

5.1.3 The service is primarily delivered remotely, using secure data transfer and processing environments. Where required, on-site support may be provided to access local systems, devices, or physical records. A hybrid delivery model may be adopted for complex or high-volume requests.

5.1.4 Typical timelines are aligned to statutory requirements, with initial scoping and data identification completed within the early stages of the response period. Progress is reviewed throughout delivery to ensure deadlines are met and to support extensions where permitted under applicable legislation.

6. Support Model

6.1.1 The DSAR Service is delivered with defined levels of support appropriate to the nature, complexity, and urgency of each request. Standard support is provided during normal business hours, with a designated point of contact assigned for the duration of the engagement to manage delivery, communications, and issue resolution.

6.1.2 Escalation paths are established at the outset of the engagement, enabling timely resolution of issues relating to scope, timelines, access, or compliance risk. Escalations may be directed to senior practitioners or service leads where required to support decision-making or manage statutory deadlines.

6.1.3 Optional enhanced support services may be provided subject to agreement, including extended hours support, expedited delivery for time-critical requests, high-volume or complex DSAR handling, and senior advisory input for legally sensitive or contentious matters. Enhanced support options are scoped and priced separately based on client requirements.

7. Exit and Offboarding

7.1.1 Exit and offboarding activities ensure the controlled and compliant conclusion of the service engagement. Upon completion, access to client systems and data is revoked, and all DSAR-related materials are securely returned, retained, or destroyed in accordance with agreed requirements and applicable data protection obligations. A final confirmation of deliverables and closure is provided, along with supporting records to demonstrate compliance, auditability, and proper handling of personal data throughout the engagement.

8. Roles and Responsibilities

8.1 Service Provider Responsibilities

8.1.1 The service provider is responsible for delivering the DSAR Service in accordance with applicable data protection legislation, agreed scope, and recognised good practice. Key responsibilities include validating and scoping DSARs, identifying and processing in-scope personal data, applying appropriate redactions and exemptions, maintaining secure handling of personal data, and producing compliant disclosure outputs. The service provider will maintain clear audit trails, provide regular status updates, and support escalation where risks to timelines or compliance are identified.

8.2 Client Responsibilities

8.2.1 The client is responsible for confirming the lawful basis for processing, validating the identity of the data subject, and providing timely access to relevant systems, data sources, and custodians. The client will supply accurate scoping information, confirm organisational policies and retention requirements, and review and approve disclosure decisions where required. The client remains responsible for final response issuance to the data subject and any associated communications.

8.3 Joint Responsibilities

8.3.1 Both parties are responsible for timely communication, adherence to agreed timelines, and escalation of issues that may impact delivery or statutory deadlines. Where legal or regulatory considerations arise, coordination between the service provider, client, and external legal counsel will be undertaken as appropriate to ensure compliant handling

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