Law Society of Ireland

STEP-BY-STEP GUIDANCE

DATA SUBJECT ACCESS REQUESTS (DSARS) HANDLING IN LAW FIRMS

Law Society of Ireland, Blackhall Place, Dublin 7

Tel: +353 1 881 5768 | Email: solicitorservices@lawsociety.ie | www.lawsociety.ie

Contents

STEP-BY-STEP GUIDANCE
DATA SUBJECT ACCESS REQUESTS (DSARS) HANDLING IN LAW FIRMS

1. Introduction:

This guidance note is designed to be practical. It sets out what to do when a person requests information from a law firm about data that the firm holds relating to that person under the General Data Protection Regulation ("GDPR").

What is a Data Subject Access Request ("DSAR")?

A Data Subject Access Request ("DSAR") is a request by an individual (the "Data Subject") to obtain access to personal data relating to them, and associated information (e.g., purposes, categories, recipients, retention). These requests are known as DSARs.

Under GDPR Article 4(1), personal data means "**any information relating to an identified or identifiable natural person"**. Article 15 of the GDPR provides that an individual has a **right to obtain a copy of the personal data** an organisation holds relating to them. This right of access is available to any person whose data is processed by the law firm. The right is given to "natural" persons (humans) only and not legal persons.

Timeline for compliance

Under GDPR (Article 12(3)), the law firm must respond to the DSAR "*without undue delay*" and in any event within **one month** of receiving the request. The DSAR can be in any format – email, letter or verbal. The most common format is in writing via email or hard copy letters. Law firms should carry out basic training for their team on how to recognise and deal with a DSAR.

Preliminary considerations: Are you the Data Controller?

Only Data Controllers can respond to DSARs. A Data Controller is an organisation that determines the purpose and means of processing of the personal data. Law firms are generally Data Controllers of the personal data they hold.

Some questions to ask:

- Does your law firm hold data relating to the Data Subject? AND
- Is your law firm responsible for that data – i.e. – does it make the main decisions about what data to collect, who to share it with, how long to store it etc)?

This guidance assumes that the law firm is acting as a Data Controller. A Data Processor is an entity that processes the data on behalf of the controller.

If the organisation is acting as a Data Processor, the DSAR should be forwarded to the relevant Data Controller promptly, and the Data Processor should support the Data Controller in responding under the terms of its contract with the Data Controller and under Article 28 GDPR.

Scope of Guidance

This Step-by-Step Guidance will provide a basic framework that law firms can tailor to their own needs on how to handle DSARs. DSARs may be received from clients, employees (current and former), contractors, job applicants, website users, and any other individuals whose data is processed by the law firm.

2. Validating the request

Firstly, it is important to ensure that the DSAR is valid. To validate the DSAR, you must first **confirm the identity** of the requestor to ensure the request has come from the Data Subject to whom the data relates and to prevent a data breach leading to fraud or identity theft. It is important to note that the DSAR can be in any format – email, letter or verbal. The most common format of this request is in writing via email or hard copy letters.

Confirming Identity of the requestor

It is necessary to:

- Ask for proof of identity (e.g. passport, driving licence etc) **[OR** if the Data Subject makes the request while securely logged into a customer portal or you know them e.g., they are an employee, you will not need further proof of ID].
- Ensure the ID matches the personal data held (e.g. name, email etc).

> **NB** – Keep a record of the verification checks and who performed them.

DSARs from third parties

Validating a request made by a solicitor/parent/third party on behalf of a Data Subject:

If a DSAR is submitted by a solicitor, parent/guardian or another third party, you must confirm that the third party is authorised to act for the Data Subject. Ask for written authority from the Data Subject confirming that the third party can act for them. Verify the identity of the Data Subject and where there is reasonable doubt regarding the identity of the Data Subject or authority, you may request additional information. If authority is not provided to you (or it is unclear), do not disclose personal data to the third party.

Solicitor

If a solicitor is submitting a DSAR on behalf of a client, written authority is essential. This can include a signed letter/email authorisation or engagement letter clearly instructing the solicitor to act on the DSAR, or a power of attorney/guardianship order where relevant.

Requests from Parents/Guardians

Sometimes a parent may seek to exercise the right of access on behalf of their child. While in general, children over 16 are considered to be mature enough to exercise the right of access on their own behalf, this must be assessed on a case-by-case basis. The welfare of the child must take precedence.

Acknowledge the validity of the request and setting scope of search

Once the DSAR has been validated it is important to determine the scope of the search. Generally, Data Subjects will look for specific data for a specific date range, however this is not always the case. If the Data Subject requests “all of their” data or the ask is too broad – the law firm can ask for the scope of their request to be narrowed e.g. asking the Data Subject for the names of departments/areas in the law firm with which they interacted and/or for specific dates to assist you to find the relevant information.

A **response** should be issued to the Data Subject to **acknowledge their request.** This may be in letter or email format. Please note that the **one calendar month timeline starts from the date of receipt of the request**. It is helpful to note the date when the one calendar month limit expires in your response.

If the request is very large or complex, you may need to extend the timeframe for response. You can extend the timeframe by a further two months. The reason for this must be explained to the Data Subject.

3. What constitutes personal data?

Personal data means "**any information relating to an identified or identifiable natural person.**"

What can identify a natural person

Identifiers of a person can include for example their name, address, PPS number, phone number. It can also include less obvious things like nicknames, initials or unique identifier numbers (for example employee numbers/patient numbers). **Any kind of information that could identify someone must be considered for purposes of fulfilling DSAR.**

4. Search Methods & Scope

Define the scope clearly:

Before commencing a search for Personal Data, it is important to:

- Identify the Data Subject (name, email, employee ID, etc.).
- Determine the time range relevant to the request.
- Clarify the types of data requested and systems to search (e.g., emails, HR records, call logs).

The person is entitled to their own personal data ie *any information relating to an identified or identifiable human being.* This includes information where a person isn't mentioned by name but by another identifier e.g. a client or patient number.

Search techniques:

- Use keyword searches in email systems and databases and take note of the searches undertaken:
  - Include variations of the Data Subject's name, initials, email addresses, nicknames, and job titles.
  - Depending on the system – you may use other identifiers like employee numbers or case references.
- Apply filters:
  - Date ranges
  - Specific folders (e.g., inbox, sent, archived)
  - Participants (e.g., emails to/from the Data Subject)

Systems to search:

- Email platforms (e.g. Outlook, Gmail)
- Document repositories (SharePoint, OneDrive, iManage)
- HR systems, ticketing systems
- Chat platforms (Teams, Slack)
- Case management systems
- Or any other systems that are relevant to the request

> **NB** – Note, although most records are now digital – it is important that if records relevant to the request are hardcopy that they are included in the search (e.g. medical records and original copies of materials etc).

> **NB** – It is important to maintain a log of search criteria, method and locations. This will assist the firm in ensuring that all reasonable steps have been taken to identify the data requested by the Data Subject.

5. Reviewing Emails Related to the Data Subject

What to look/search for:

- Emails sent to or from the Data Subject
- Emails mentioning the Data Subject, even if they're not a sender/recipient
- Attachments containing personal data (e.g., performance reviews, contracts)

Details to include:

- Full email content (subject, body, metadata like timestamps)
- Attachments (if they contain personal data)
- Contextual threads if relevant to understanding the message

Check list:

Include emails:

- Sent to/from the Data Subject and **relating to them personally** - there is no need to include every email an employee sent when fulfilling his/her role as an employee. However, you must include emails that relate to that employee personally e.g. if their behaviour or performance is mentioned etc
- Mentioning the Data Subject personally (as above)
- With attachments containing personal data

And:

- Include metadata (date, time, sender, recipient)
- Include relevant threads for context
- Exclude irrelevant or duplicate emails

Exclude:

- Emails unrelated to the Data Subject
- Duplicate content unless contextually necessary

6. Redaction Guidelines

The Law firm must provide the Data Subject with a copy of their personal data (Article 15(3) GDPR). However, the **right of access is not absolute** and there are restrictions to the right provided in the GDPR and the Data Protection Act 2018.

Once you have completed your searches and have gathered all relevant related information, it is important to redact information that the Data Subject is not entitled to.

First, make a copy of all the relevant information:

- If the document is in soft copy form, download and save a separate version of this file as your "working copy".
- Redaction should only be carried out on the working copy, never on original documents.

It is important that the person carrying out the review and redaction exercise understands the nature of the documents that are being reviewed. The Data Protection Commission advises that the person responsible for preparing the DSAR must "*be sufficiently familiar with the material being examined to recognise data identifying the Data Subject, and equally importantly, data identifying other individuals".*

Please see **Schedule 1** for a list of the relevant restrictions contained in the GDPR and the Data Protection Act 2018. Certain health and social work data my need to be checked with a clinical expert before release to ensure it won't cause harm to the Data Subject (Data Protection & Access Modification Health/Social Work Regulations).

Key Steps

- Start with disclosure: identify what is clearly the requester's personal data and is in scope, based on the request made.
- Apply restrictions only where necessary and proportionate and document the legal basis and reasoning.
- Redact narrowly: remove only what must be withheld, unless the document is non-personal or cannot be safely separated.
- Always keep a Redaction Log / Decision Log (what was withheld/redacted, why, and under what legal basis).

Key Restrictions for law firms

The key restrictions are outlined in **Schedule 1** and **Schedule 2.**

Other important considerations for redaction:

Co-Mingled Data

Where the Data Subject's personal data appears in the same record as a third party's personal data (e.g., a complaint email naming multiple individuals or a meeting note referencing colleagues) this is known as comingled data. In these scenarios, you should disclose as much of the Data Subject's personal data as you can while protecting the third party's rights. Always err on the side of caution. It is better to refuse release (as long as you can justify it) than release it and cause harm. For co-mingled data:

- Redact third-party identifiers (names, contact details, unique roles) where disclosure would identify the third party.
- If the third party's identity is obvious from the context of the document, even after name redaction, redact the wider sentence/paragraph or summarise the Data Subject's personal data instead.
- If the third-party information was provided by the Data Subject and they are already aware of it (e.g., they wrote it or already have a copy of it), redaction may not be necessary but assess on a case-by-case basis.
- If safe separation cannot be achieved, you may withhold the record and explain the reason in the schedule/cover letter (Article 15(4) balancing).

7. Technical Measures for Redaction

Best practice

- Use professional redaction tools (PDF editors, DMS with redaction features).
- Combine all "working copy" documents into one PDF (or request the client sends the documents to us in this format). If there is a large volume of documents, you may need to create more than one PDF.
- Make the redactions on this PDF, saving the original documents for reference purposes.
- Ensure redacted content is fully obscured and not recoverable (see below).
- **Keep a copy** of the original and redacted versions for audit trail.

You must ensure:

- Redactions are complete and irreversible.
- Files are named clearly and consistently.
- A **copy of the original (unredacted) version is retained securely for audit purposes**.
- Use the tools, including **sanitising the document to remove hidden data** and metadata.

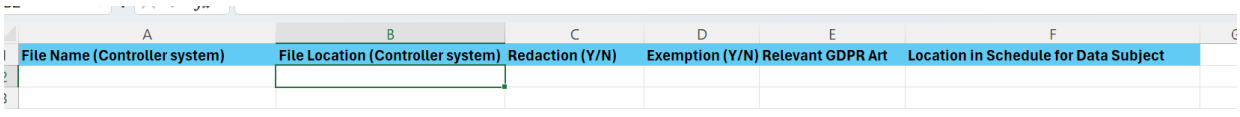
Redacting Hard copy related documents

Hardcopy documents should be scanned, copied and converted to PDF. Once you have a digital copy of same, repeat processes above to ensure all relevant information and data is redacted.

Recording Document Redaction methods and decisions

It is important to record and maintain a log of what information has been redacted and the reasons for the redactions (including the restriction applied from the GDPR/Data Protection Act. e.g. GDPR Article 15 (4) adverse impact on the rights and freedoms of others etc (see **Schedule 1**). The Irish Data Protection Commission's ("DPC") guidance specifically states that "*any restriction of the right of access or to information must be justified on an evidential basis, by reference to the specific context of the case concerned".*

A spreadsheet can be a helpful mechanism to keep track of the redactions applied and the restriction relied upon when applying this redaction.



A	B	C	D	E	F
File Name (Controller system)	File Location (Controller system)	Redaction (Y/N)	Exemption (Y/N)	Relevant GDPR Art	Location in Schedule for Data Subject

This log is also essential for audit trail purposes should the DPC request the justification and reasoning for not providing or redacting some information.

8. Quality control

- Conduct a second-person review for high-risk cases (large volume, sensitive data, significant third-party content, legal proceedings).
- If there is litigation involved, ensure that the legal team is fully briefed on what documents have been released to the Data Subject.
- Check that redactions are irreversible (cannot be copied/recovered).
- Check that no hidden content remains (metadata, tracked changes, embedded files).

9. Preparing the Response

Once all relevant Personal Data has been identified, reviewed, and redacted appropriately, the final step is to securely provide the documentation to the Data Subject. This step must be handled with care to ensure compliance with GDPR and to maintain transparency and trust.

DSAR Fulfilment letter

A DSAR fulfilment letter is the formal communication responding to the DSAR and summarising the restrictions applied.

It should include:

- Confirmation of the identity verification process.
- A summary of the types of data provided.
- Any limitations or redactions applied, with brief justifications.
- The date of the original request and the response date.
- Contact details for follow-up or complaints (e.g., DPO or relevant authority).
- Reference to the right to lodge a complaint with the supervisory authority.

As per the guidance from the Data Protection Commission, the Data Subject is entitled to additional information about the processing of their data.

This includes:

- Purposes of the processing
- Categories of personal data processed
- Who the personal data is shared with
- How long the personal data will be stored
- Existence of Data Subject rights
- Right to lodge a complaint with the Data Protection Commission
- Information about where collected from
- Existence of automated decision making
- Safeguards in place if transfers to 3rd countries or international organisations occur.

Schedule of Documents

A schedule of documents is a structured index or table listing all documents included in the response. This helps the Data Subject understand what has been provided and where to find specific information. If the response to a request is very long, a description of redacted information may be used instead. Please note that the DPC sometimes requests that Data Controllers provide a full Schedule of redacted information. This is good practice but is not required under GDPR, and some organisations will push back on this point.

If you provide a schedule, check that the schedule and cover letter match the released files and page counts.

10. Delivery of documents to Data Subject

Secure Delivery Methods

Choose a secure method of delivery based on the sensitivity of the data and the preferences of the Data Subject. It is best practice to password protect the folder containing the data. The password should not be included as part of the delivery of the data. It should be sent separately. These procedures should all be agreed in advance with the Data Subject.

Physical Delivery

If you have agreed to provide the personal data in hardcopy format, the information should be sent using tracked and signed-for delivery services or collected by the Data Subject.

Always confirm the preferred method of delivery with the Data Subject and document this choice.

11. Final Checklist Before Sending

- Identity verification completed and logged
- Request scope confirmed and documented
- All relevant systems searched
- Redactions applied and logged
- DSAR Fulfilment letter and schedule prepared
- Secure delivery method confirmed
- Audit trail maintained

Schedule 1:

Relevant restrictions to consider where fulfilling a Data Subject access request:

Restriction	Legal basis	When it may apply	Examples / practical note
Data must be the requester's personal data (not general documents)	GDPR Art. 4(1), Art. 15(3)	Where a document contains no personal data about the Data Subject.	Policy documents are attached to an email thread but not relating to the Data Subject = withhold as non-personal.
Rights and freedoms of others (third-party data) and disclosure would cause an adverse effect on the third party	GDPR Art. 15(4)	• Where disclosure would identify another individual and that disclosure is likely to adversely impact their rights. • If releasing Confidential business information (e.g. trade secrets, financial data) would cause an adverse effect.	• Personal data that can directly or indirectly identify another person (for example name, job title, initials, contact details) **if** releasing that information is likely to adversely affect that person. • Confidential business information e.g. proprietary protected IP.
Security-sensitive information	GDPR principles (security), Art. 32; Art. 15(4) balancing	Where disclosure would compromise security or enable unauthorised access.	Passwords, access codes, vulnerability details = redact/ withhold.
Cabinet confidentiality/ parliamentary/ national security/ defence/ international relations	Data Protection Act 2018 (Ireland) ("DPA 2018"), s. 60(3)(a) (i)	Where it is essential to safeguard cabinet confidentiality, parliamentary privilege, national security, defence and international relations of the Irish state.	Documents referencing Cabinet discussions, confidential government briefings = redact/withhold.
Criminal offences	DPA 2018, s. 60(3)(a) (ii)	Where disclosure would impact the prevention, investigation, detection or prosecution of criminal offences, prevention of threats to public security or the execution of criminal penalties.	Draft or submitted reports to Gardai/ regulatory bodies if disclosure would undermine investigation steps or expose confidential sources = redact/withhold.
Tax administration	DPA 2018, s. 60(3)(a) (iii)	Where disclosure would be likely to prejudice the state or local authority's tax administration.	Internal Revenue notes that could undermine ongoing tax administration if disclosed = redact/withhold

Restriction	Legal basis	When it may apply	Examples / practical note
Legal advice & privilege; contempt of court	DPA 2018 s. 162	Privileged communications and where disclosure would be contempt of court.	Email chain with external solicitors giving legal advice = withhold/redact in full. Internal documents discussing strategy in a court case = withhold/redact in full.
Information in contemplation of or for the establishment, exercise or defence of legal proceedings.	DPA 2018 s. 60(3)(a) (iv)	Where disclosure would compromise the establishment, exercise or defence of, a legal claim or a potential legal claim.	Pre-action legal strategy notes (internal or from counsel). Draft legal proceedings prepared for a claim where disclosure would reveal legal strategy = redact/withhold
Information that could affect the enforcement of civil claims	DPA 2018, s. 60(3)(a) (v)	Information relating to any liability of a controller or processor in respect of damages, compensation or other liabilities or debts related to the claim	Eg assessments of liability = redact/withhold
Estimation of amount of liability	DPA 2018, s. 60(3)(a) (vi)	Where disclosure may prejudice the commercial interests of the data controller where a claim has been received	Insurance communications: reports to insurers estimating liability/compensation (where disclosure would prejudice commercial/legal position) = redact/withhold
Expression of opinion given in confidence	DPA 2018, s. 60 (3) (b)	Opinion about the requester provided confidentially by another person with a legitimate interest in receiving information.	Confidential whistleblowing report identifying the requester = consider withholding/redaction with justification.
The Information Commissioner or the Comptroller and Auditor General	DPA 2018, s. 60(3)(a) (c)	Information relating to the performance of their general functions are excluded from Data Subject access requests.	N/A
Health data: serious harm (context-specific)	Irish Access-modification Regulations (Health)	Where release would be likely to cause serious harm to the requester's physical or mental health.	Sensitive diagnosis not previously disclosed = seek clinical consultation; consider staged disclosure via clinician. Consult appropriate health professional
Social work data: serious harm (context-specific)	Irish Access-modification Regulations (Social Work)	Where release would be likely to cause serious harm to health/emotional conditions.	Detailed trauma narrative in social work report = consult appropriate professional; redact/withhold

Schedule 2: Limitations

Limitation	Legal basis	When it may apply	Example / practical note
Identity verification where reasonable doubts exist	GDPR Art. 12(6)	Where the organisation cannot be confident that the requester is who they claim to be.	Email from a new address requesting *"all my data"* with mismatching details = request ID.
Manifestly unfounded or excessive	GDPR Art. 12(5)	Repeat requests with no reasonable interval, harassment, or disproportionate burden.	E.g. repeated requests with no change "Send me everything again" two weeks after you already provided the full response with no new scope or change.
Extension for complex/ numerous requests	GDPR Art. 12(3)	Complex searches, multiple systems, high volume, and legal review needs.	Large case file + multiple third parties = extend up to 2 months; notify within 1 month.

Schedule 3: Practical redaction examples

Use these examples to drive consistent decisions and to document reasoning in the Redaction Log. Add in more examples as common issues arise.

Example record	Risk/issue	Suggested approach
Meeting notes: *"KayKay raised a complaint about John's conduct and said Mary witnessed it."*	Co-mingled third-party data; context may identify John/ Mary even if names removed and could adversely affect John/Mary.	Keep the requester's personal data. Redact third-party names and unique identifiers. If still identifiable, redact the wider sentence or provide a short summary of the requester's personal data.
Email: "Please reset KayKay's account. Temporary password is X."	Security credentials.	Disclose that an account reset occurred (if it is the requester's data) but redact the password and any security answers.
HR document listing multiple employees' salaries including requester.	High-risk third-party data.	Extract and disclose only the requester's line/record (or produce a redacted copy where others are fully removed).
Customer support ticket includes the requester's message plus agent notes about internal fraud checks.	May involve confidential sources/methods and third-party identifiers.	Disclose the requester's message and outcome. Redact internal identifiers, third-party data, and any method details where disclosure would undermine security or others' rights.

Annex 1: Checklists, logs and templates

A1.1 DSAR Handling Checklist

- [ ] Request received and saved (original preserved)
- [ ] Case logged on DPO Dashboard and team assigned
- [ ] Acknowledgement issued; deadline diarised
- [ ] Identity/authority verified (or not required; rationale recorded)
- [ ] Scope clarified with Data Subject (if needed) and recorded
- [ ] Search plan agreed; system owners assigned
- [ ] Search log completed, stored and documented
- [ ] Dataset prepared (dedupe, convert, hidden content checks)
- [ ] Restrictions assessed; redaction log completed
- [ ] Cover letter drafted (includes required information)
- [ ] Schedule of documents prepared
- [ ] Quality Control completed (second person review if high risk)
- [ ] Secure delivery method confirmed; details re-verified
- [ ] Response sent; release recorded
- [ ] Case closed; evidence pack retained per retention schedule
- [ ] DSAR Log updated to reflect date sent.

A1.2 Logs to maintain

- [ ] DSAR Log/Tracker: key dates, owner, status, delivery method, closure date
- [ ] Search Log: systems, keywords, date ranges, evidence of reasonable searches
- [ ] Redaction/Decision Log: what withheld/redacted, legal basis, necessity/proportionality notes
- [ ] Disclosure pack index (schedule of documents)

This resource was developed by Pembroke Privacy in consultation with the Law Society of Ireland.

Law Society of Ireland,
Blackhall Place,
D07 VY24
E solicitorservices@lawsociety.ie
W www.lawsociety.ie