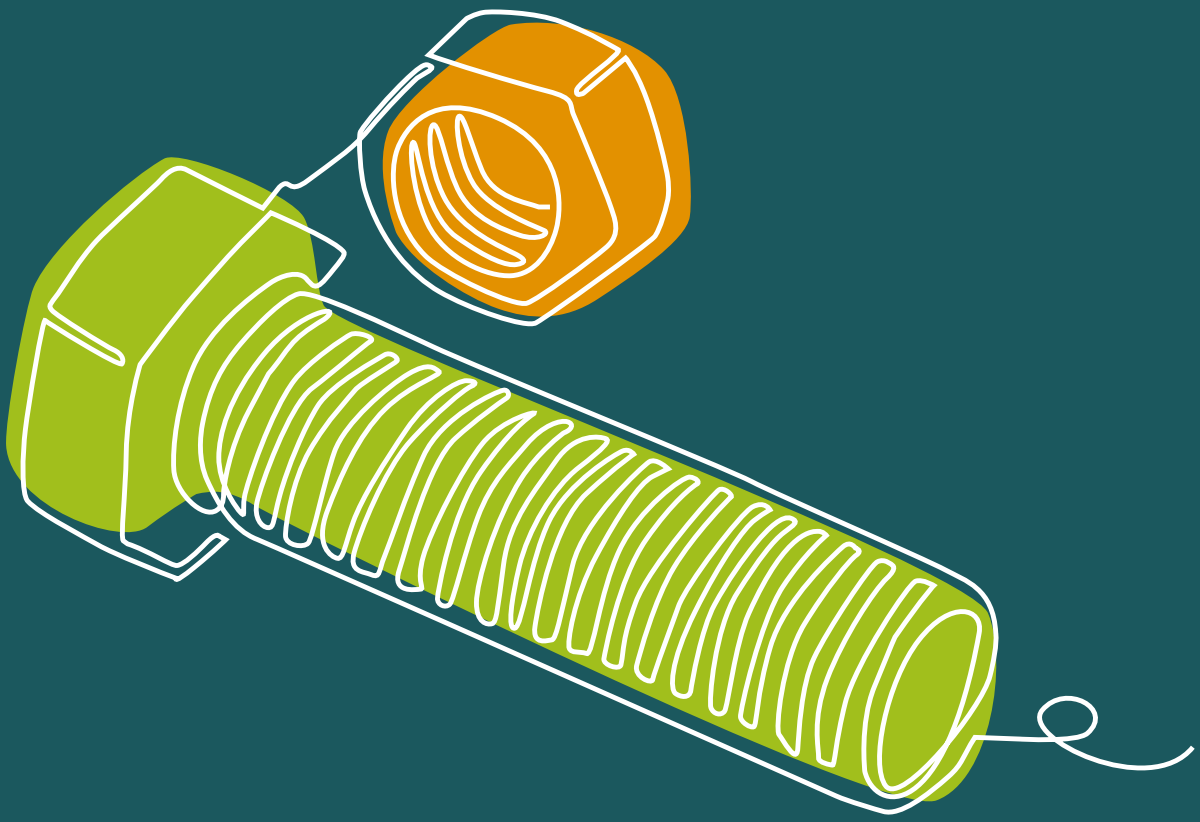
GUIDE TO DATA SUBJECT ACCESS REQUESTS

The Nuts and Bolts



Being prepared & handling DSARs

Publication date: April 2022

Sponsored by exterro®

DPN
DATA PROTECTION NETWORK

Contents

Foreword

Handling Data Subject Access Requests ("DSARs" or "SARs") can be daunting, complex and time-consuming. Whether you receive a hundred requests a month or one a year, your organisation needs to be able to fulfil people's fundamental 'Right of Access'.

Careful planning, adequate resources and sufficient understanding are essential for responding within the tight legal timeframe.

The DPN's data protection consultants have for a number of years been supporting businesses across a range of sectors to handle DSARs. We understand the difficulties they can pose. We appreciate how nuanced they can become and how tricky employee-related requests can be.

DSARs are a topic frequently covered in our articles and webinars, as well as a hotly debated topic in our Advisory Group meetings.

The UK Government's Autumn 2021 data reform consultation paper recognised the burden of DSARs, especially on small-to-medium sized organisations. Changes being considered include introducing a cost limit modelled on the Freedom of Information Act, amending the threshold for vexatious requests and re-introducing a nominal fee.

This guide aims to help you to be prepared, understand the workflows involved, provide the specialist knowledge required and other key considerations.

This guide is aimed at UK organisations, but may be of interest to those in other territories. It is not exhaustive and we would stress DSARs are an area where professional views can vary and different approaches are taken. If you are unsure, we would always recommend seeking internal or external specialist advice.

Robert Bond

Chair of Advisory Group
Data Protection Network
www.dpnetwork.org.uk

Executive summary

DSARs are a key data protection challenge

A recent DPN survey showed DSARs to be one of the key challenges facing DPOs and those responsible for data protection. Volumes can fluctuate, the scope is broad, and they can be resource intensive. Employee-related requests can be particularly challenging, where other factors such as unfair dismissal claims are in play.

Being unprepared is no excuse

People's right to request a copy of their personal data has been a core part of UK and EU data protection law since the 1980s. Regulators would expect robust measures to be in place to fulfil requests. Staff should know what requests 'look like' and how to escalate them. Organisations need to know where their data is. Teams handling them should be sufficiently knowledgeable and adequate resources need to be allocated to handle them within a tight legal timeframe.

The 'weaponisation' of DSARs

Organisations may believe an individual making a request has an ulterior motive. In general, the motive should not impact on the person's fundamental right of access. Some requests may be clearly vexatious or excessive, but the criteria to meet this threshold is high. Organisations will need a sound justification for not fulfilling a DSAR, either partially or fully.

The careful balance of 'complex' requests

It's permitted to seek clarification when a request is considered 'complex' and in such cases the timeframe for responding may be extended. The onus is on organisations to judge this and be able to demonstrate why a specific request is complex not routine.

The data retrieval process

Organisations are expected to make all reasonable efforts to search, identify and retrieve all the personal data requested. Systems need to be well-designed to enable data discovery and retrieval. You'll need to be able to justify if a specific search would be unreasonable or disproportionate.

Applying redactions and exemptions

Sufficient time needs to be factored into the process to redact certain information, which for example may relate to others or be commercially sensitive. Organisations need to be able to effectively apply redactions. An understanding of how certain exemptions may apply and relate to your business is crucial.

Technical solutions can streamline the process

Time and cost efficiencies can be made by developing in-house solutions or using external technical solutions to streamline the process. There are a range of solutions on the market which cover the end-to-end process or specific aspects such as data discovery, retrieval or redaction.

1. Introduction

People's right to request a copy of their personal data, from both private and public sector organisations, has been part of UK data protection law since the 1980s. Awareness has grown in recent years, largely driven by GDPR.

This has led to many organisations seeing a significant rise in the number of requests or receiving requests for the first time. Some have streamlined their processes, perhaps using automated tools. Others take a more manual approach.

While some DSARs can be relatively straight-forward, others are more complicated and difficult to handle. The following can play a part in dictating the level of complexity:

- The nature of your business
- The nature of the request
- The nature of your relationship with the individual

Challenges

In our *Privacy Pulse Report 2022*, people working in data protection revealed the following key challenges when handling DSARs:

Key DSAR Challenges

Identifying requests	recognising DSARs within the organisation
Resources	specialist skills and time needed to process requests
Email searches	retrieving and reviewing email correspondence
Redaction	what to redact and how to do it
Systems	accessing relevant systems across the organisation
Scope	the broad 'all of my personal data' scope
Volume	sheer volume of records
Time	responding within the legal timeframe
Weaponisation	ulterior motives

Context of the request

Often the nature of your relationship with the individual, and what may have led them to submit a request, can make requests more difficult to process.

Angry customer

- Disputes process for verifying their identity
- Misunderstands what they're entitled to
- Threatens to escalate a complaint

Disgruntled former employee

- Intends to submit unfair dismissal or discrimination claim / impending tribunal
- Large volume of data, due to many years' employment

While it's important to fully understand the context of a request, you need to strike the right balance. An individual's motive unless clearly vexatious should not impact on their rights.

> *"As the person managing the request, it is important to ensure that the subject access process is not unduly influenced by these broader customer or employee matters but kept separate; thereby preserving the integrity of the subject access process and impartiality and independence of the DPO."*
> **Michael Bond | Group Data Protection Officer | News UK**

Case Law

There's no limitation on the purposes for which an individual may request their personal data via a DSAR. Another purpose, such as using personal data to assist in litigation, isn't of itself a justification for refusing to comply.

Dawson-Damer vs Taylor Wessing LLP, 2017

Risks

If someone isn't content with your response, they could take legal action or escalate their complaint to the Information Commissioner's Office (or other applicable Supervisory Authority).

A staggering 46% of all the complaints the ICO received in 2019 related to DSARs. *(Source: ICO Annual Report 2020/21)*

The risks organisations face include:

- Disclosing information in error
- Failing to provide all in-scope personal data
- Failing to respond in time
- Rising costs
- Lost time

If regulatory complaints are not resolved satisfactorily, it could lead to unwelcome scrutiny of more than just your processes for handling individual rights requests and extend to your data protection practices more broadly.

2. What the law requires

2.1 What's a DSAR?

The Right of Access is a fundamental right under data protection law in the UK and European Union, and in some other jurisdictions.

- Requests are commonly referred to as a Data Subject Access Request ("DSAR" / "SAR").
- Under EU / UK GDPR people have the right to receive a copy of their personal data from any organisation acting as a Controller.
- Suppliers, acting as Processors, are required to assist Controllers, as and when necessary.
- The legal purpose of a DSAR is to make sure people can check their information is being handled lawfully and get a copy of what an organisation holds about them.

2.2 What people are entitled to

People are entitled to a copy of their personal data and other supplementary information.

Checklist for DSAR entitlement

- ✓ Confirmation the organisation is processing their personal data
- ✓ A copy of their personal data
- ✓ Other supplementary information

What is meant by a 'copy of personal data'?

People should receive a copy of information which could directly or indirectly identify them. Personal data could include contact details, images, voice and video recordings, demographic information, profiles, order history, marketing preferences, HR records, opinions expressed about the individual, other personal identifiers such as employee number and so on.

Case Law

Controllers can't refuse to disclose information when responding to a DSAR on the grounds that this information will not tell the individual anything they didn't already know. Information already known to the individual is within the scope.

Lttihadieh v 5-11 Cheyne Gardens, 2017

Other supplementary information

Along with a copy of their personal data, the 'other supplementary information' includes explaining the purposes you are using the person's data for and how long you envisage keeping records for.

Where this information is clearly available in your Privacy Notice, it's sufficient to provide a link to this in your DSAR response. Full details of the supplementary information can be found in the *ICO Right of Access Guidance.*

What is out of scope?

- **Full documents**
  A DSAR isn't a right to documentation. Just because someone's name appears in an email, report or letter doesn't mean they're entitled to the whole document. It may be easier and relevant to provide full documents, but equally you may be justified in not doing so.
- **Anonymised data**
  If personal identifiers have been removed from a dataset, and it's truly anonymised, it no longer falls under the scope of data protection law.
- **'Loose' notes**
  Personal data which is not part (or intended to be part of a structured filing system) is not in scope. For example handwritten notes in a personal notepad where there's no intention to formally file these notes would not need to be included.

3. Core building blocks

3.1 Informing people of their rights

You need to tell people about their privacy rights, such as the right to object, right to rectification, right to erasure and right of access (etc.)

- ✓ This information should be in your privacy notice
- ✓ It should be clear how people can submit requests

Some organisations use specific DSAR forms, or a dedicated portal, but you can't force people to use these. You also can't routinely charge a fee.

3.2 Recognising requests

Staff need to be alert how people might submit requests and what they might 'look like'.

- Requests are valid by email, letter, over the phone or even via social media.
- Requests do not need to be submitted to a specific person or department to be valid.
- A request doesn't need to say 'data subject access request' or 'right of access' to be valid. Nor does it have to reference GDPR or the Data Protection Act.

A DSAR is when people ask you to provide them with the personal data you hold about them. Sometimes this request may come from someone else on the individual's behalf. People may also mistakenly reference the Freedom of Information Act (FOI), when they meant to request a DSAR. The onus is on organisations to identify and interpret the requests received.

What about routine requests for information?

Some requests for information can be handled routinely and don't need to be treated as a DSAR.

- requests for bank statements, payslips, order information or telephone recordings may be routine depending on the nature of your business.
- If someone asks where their personal information was sourced from, or why you are sending them marketing, this may be handled in a routine manner.

Unless, of course, they're also asking more broadly for the information you hold about them.

> *"Who should be at the front line, and equipped to answer DSARs? The people who most routinely interact with customers, the customer support staff who your customers first interact with."*
> **Ray Pathak, Vice President Data Privacy, Exterro**

3.3 Training and awareness

It's important to train staff to be able to recognise DSARs and know what to do if they receive one.

Good practice training and awareness checklist

- ✓ Individual privacy rights are covered in new starter and refresher training
- ✓ Ongoing awareness via posters, intranet posts, newsletters etc.
- ✓ Specialist training for those involved in the process of fulfilling requests

3.4 Knowing where your data is

You won't be able to effectively respond to a DSAR if you don't know where personal data is and don't have systems enabling you to locate and extract personal data. Organisations are expected to have both robust procedures and the technical ability to fulfil requests.

Where's my data - key questions

- Where is personal data located?
- Will searches differ depending on who is making the request (e.g. customer, client, donor, patient, employee etc.)?
- Consider if any paper filing systems are relevant for the request.
- Do suppliers (processors) need to be involved?

An Information Asset Register which states where and how you store personal data can help speed up the process. An up-to-date Record of Processing Activities can also prove helpful when you need to establish which systems are relevant to a specific request and what purpose you're processing if for (to fulfil 'other supplementary information').

3.5 Unstructured data challenges

Searching unstructured systems can prove particularly time-consuming. Such as email systems and other internal messaging systems.

Unstructured data - key questions

- Do our systems enable us to search for specific personal data?
- Can a method be developed for excluding routine business-as-usual messages?
- Can automated tools be used to identify personal data?

3.6 Resourcing

Organisations receiving a significant volume of requests are likely to have a dedicated team to handle them. Others with lower or fluctuating volumes may find it difficult to know how much resource is needed. Plans need to cover holiday or sick leave. Also, bear in mind the one calendar month response time can't be extended due to bank holidays. It can pay to be well-prepared for Christmas DSARs.

You'll also need to factor in how to handle a predictable or random spike in requests. Have you got other adequately trained staff, or alternative resources on standby to cover higher than routine volumes?

3.7 Allocating responsibility

While one person or team may have ultimate responsibility for the 'project management' of DSARs, they're likely to need to rely on others across the business to support them. The IT team is likely to play a significant role in retrieving the data, but others will too. You need to be able to allocate roles to specific people or teams.

Do you know who'll be responsible for...

- Project managing DSAR responses?
- Retrieving the data?
- Reviewing the data?
- Applying exemptions?
- Applying redactions?
- Reviewing final response?
- Approving response?

It may not always be the Data Protection Officer, or the person responsible for data protection, who handles requests. Some businesses may choose to assign responsibility to other teams. The HR team may, for example, be responsible for handling employee-related requests.

3.8 Having a clear procedure

A robust procedure can help walk staff through the key steps and considerations.

Example - DSAR procedure contents

Recognising requests
Staff awareness and training.

Confirming receipt
Logging requests, acknowledging, clarifying nature of request, id verification, clarifying scope and diarising.

Can the request be refused?
Is it manifestly unfounded or excessive? Can it be fully or partially refused?

Retrieve the data
Confirm the search criteria and search terms. Issue search requests.

Collate and assess
How to treat personal data relating to others. Considering other exemptions that may apply.

Redaction
Apply redactions (and/or extract personal data where full documents are not being disclosed).

Compose, review and approve response
Prepare a covering letter, review response and gain approval.

Send response securely
Send response by a secure method and in a format agreed with the individual.

Close request and retain documentation
Retain records, including justification for any decisions taken. Apply appropriate retention periods.

4. Getting started once a request is received

4.1 Initial steps

Any requests received should be logged and the person informed their request has been received. You may need to clarify the nature of the request if it's not clear, or simply inform them that you don't process any of their personal data.

Organisations will take varying approaches to how they initially handle a request. If the process is automated this may dictate the steps to take.

DSAR receipt - standard checklist

- ✓ Log receipt of request
- ✓ Acknowledge request
  - Is proof of ID required?
  - Does another party have authority to act on the individual's behalf?
  - Is the nature of the request clear (are other rights, such as erasure or right to object being requested as well)?
  - Does the scope need clarifying?
  - Can the request be refused?
- ✓ Diarise response data
- ✓ Agree with individual format for response (e.g. paper or electronic)

A request can be refused in part, or fully, where it is judged to be 'manifestly unfounded' or 'manifestly excessive'. For more detail on this please see **Vexatious or excessive requests**.

4.2 When the clock starts ticking

Unless it's particularly complex, you need to respond to a DSAR within one calendar month.

- The clock starts once you have validated the individual's identity.
- If you need to clarify a request, you can 'pause the clock' from the day you ask the clarifying question(s) to the day you receive a response.
- If a request is judged to be complex you can extend the timeframe by up to a maximum of two further months.

"The earlier and more effectively you satisfy a Data Subject Access Request, the less likely it will become a complaint and require escalation."
Ray Pathak, Vice President Data Privacy, Exterro

4.3 Validating identity

Where someone's identity is obvious, for example a request from an employee, it may not be necessary to request proof of their identity. If you have any doubts about the identity of a person, you can take reasonable steps to confirm they are who they say they are.

Organisations need to be alert to people attempting to impersonate and the use of deception to access to information. However being over-zealous and insisting on excessive forms of identification can raise objections. It could be seen to be putting an unnecessary barrier in people's way.

4.4 Seeking authorisation

Where someone submits a request on behalf of another person, you need to be sure the request is genuine. Has the individual agreed to this, and does the third party have authority to act on their behalf? Steps you can take include:

- Request proof of power of attorney.
- Seek explicit authority to act on the individual's behalf.
- Contact the individual the request relates to and ask them to confirm they're happy for you to proceed.

People may not be fully aware of the nature and sensitivity, or indeed volume of personal data which may be shared with the third party.

Third party online portals

In recent years a number of online portals have been developed which offer to submit DSARs on behalf of consumers. While this is a positive step for consumers, these portals should be treated with a degree of caution. Steps you can take include:

- Validate the identity of the individual the request relates to.
- Make sure the portal has the authority to act on their behalf.
- Conduct due diligence if response is to be submitted via the portal.

> *"Once your organisation has been identified by an online portal, you could receive multiple requests. I once had 9,000 in my inbox in one hit. While this may be extreme, it's important to have robust procedures to enable you to identify legitimate requests and respond accordingly."*
> **Chris Field, Corporate Privacy Director, Harte Hanks**

You may decide an appropriate approach is to contact the individual in question to confirm their request before proceeding. You may also decide it would be best to provide your response directly to them, rather than via the portal.

4.5 Complex requests

The ICO says you can seek clarification where a request is considered 'complex' and you can potentially extend the timeframe for responding for up to a maximum of a further two months.

When is a request complex?

The law doesn't tell us what makes a request complex. Organisations need to judge this based on all the facts of a specific case. You'll need to be able to demonstrate why a request is particularly complex for you to handle.

> *"Requests that involve a large volume of information may add to the complexity of a request. However, a request is not complex solely because the individual requests a large amount of information."* **ICO Right of Access Guidance**.

Factors which may add complexity

- **Technical difficulties** - for example, retrieving data from an electronic archive.
- **Applying an exemption** – for example, involving large volumes of sensitive information.
- **Specialist work** – for example, retrieving or providing the information in an intelligible form.
- **Confidentiality** – for example, clarifying whether sensitive medical information can be disclosed to an authorised third party (where a request has been submitted by this party on behalf of the individual).
- **Specialist advice** – for example, needing to obtain non-routine specialist advice.

4.6 Seeking clarification

If a request isn't clear, or the request relates to a large volume of data, you can ask the individual to clarify their request. The ICO tells us clarification shouldn't be sought on a blanket basis.

You can ask, but you can't force someone to narrow the scope of their request. Individuals are fundamentally entitled to ask for all the information you hold about them.

5. Vexatious or excessive requests

Sometimes it may be clear an individual has an ulterior motive for submitting a DSAR. In general, an individual's motives should not affect their right to obtain a copy of their personal data, or the organisations duty to respond.

However, organisations can refuse to comply, either partially or fully, where they judge a request to be 'manifestly unfounded' or 'manifestly excessive'. You'll need a clear justification to rely on these grounds.

It's also worth noting you're only permitted to charge a 'reasonable fee' to cover administrative costs in responding to a DSAR when it is judged to be manifestly unfounded, excessive or if further copies are requested.

Manifestly unfounded – questions to consider

- Is it clear the individual has no intention to exercise their right?
- Has the individual offered to withdraw their DSAR in return for some form of benefit?
- Has the individual explicitly stated they want to cause disruption?
- Has the individual made unsubstantiated accusations or allegations?
- Is the individual targeting a specific employee due to a grudge?
- Has the individual sent regular and different requests as part of a concerted campaign?

Manifestly excessive – questions to consider

- Is the request clearly or obviously unreasonable?
- Will the request involve disproportionate effort?

6. Data retrieval

Before issuing search requests to relevant teams you'll need to confirm the search terms and relevant systems.

- Organisations are expected to make all reasonable efforts to search, identify and retrieve all the personal data being requested.
- Systems should be well-designed and maintained so information can be efficiently located and extracted.
- Taking account of the importance of the information requested, you're not required to conduct searches which would be clearly unreasonable or disproportionate.

Archived records and back-ups

The ICO says there's no 'technology exemption' when responding to a DSAR. Just because accessing electronical archives or back-ups may be more complicated, this doesn't render them out of scope.

Deleted records

If records have been deleted, and you've no intention of accessing them again, the ICO says you are not required to go to the extensive technical effort of recreating this data.

7. What to redact or exclude

Once the searches are completed, you need to collate and assess the information retrieved. This can be one of the most time-consuming aspects of the process. You'll want to allow enough time for this stage so it's not unduly hurried.

Key considerations include (but are not limited to):

- Protecting the privacy of others
- Protecting the intellectual property of your business
- Maintaining confidentiality
- Potential conflict with other legal obligations
- Avoiding over redaction

7.1 Information relating to other people

The person making the request has a right to receive a copy of their personal data, they're not entitled to personal data relating to other people.

Some of the information retrieved may include personal data relating to other individuals, or information that could identify other people. For example:

- Employees
- Family members
- Individuals who have expressed opinions about the requester
- Individuals who have made allegations against the requester

The UK Data Protection Act 2018 confirms you do not need to include certain information if it means disclosing information which identifies someone else, unless:

- The other person has given their consent
- It's reasonable to disclose without the other person's consent

Information relating to others – key questions

- Can it be removed or redacted?
- Is it appropriate or possible to ask for consent?
- Has consent been refused?
- Is the information sensitive?
- Is it fairly innocuous and reasonable to disclose without consent?
- Is there a duty of confidence?

It is likely sensitive or particularly private information relating to other people will need to be redacted or removed. However, personal data routinely shared as part of everyday business, such as the names or business contact details of people in their professional roles (unless commercially sensitive) are unlikely to have a severe consequence if disclosed as part of a DSAR. Decisions will need to be taken on a case-by-case basis.

Example – unredacted information relating to others

In an employee related DSAR the data retrieved contains names and email addresses of other members of staff. The parties are all known to each other and in the context, this does not unduly impact on the privacy of current staff. A decision is taken not to redact this information.

7.2 Confidential information

A duty of confidence may arise when another individual has genuinely shared 'confidential' information with the expectation that it remains confidential. Confidentiality cannot be automatically assumed and needs to be assessed on a case-by-case basis. Other information which may also be considered confidential includes:

- Trade secrets
- Information made confidential under another law
- Internal costs or commercial rates
- Intellectual property
- Information covered as part of a non-disclosure agreement

7.3 Considering other exemptions

The Data Protection Act 2018 provides a number of further exemptions which may apply depending on the nature of your business and the context of the specific request. It's worth noting:

- The exemptions exist to cover the fact organisations may have legitimate reasons for not disclosing certain information.
- The exemptions don't always apply in the same way, and some may never be relevant to your business.
- Sometimes you are obliged to rely on an exemption (i.e. it would break another law), other times you can choose whether to rely on an exemption or not.

> *When considering what your DSAR response will consist of, you will need to understand what information a data subject is legally entitled to and when information can legitimately be withheld. If information is to be withheld, then it is important that you clearly document internally what information is to be withheld and what exemption you are relying upon.*
>
> *Your DSAR Team will need to be trained as to how exemptions apply and understand the nuances of the Data Protection Act 2018. This will assist you when responding to any requests for clarification from the ICO or further correspondence from data subjects.* **Chris Whitewood | Privacy & Data Protection Officer | Direct Line Group**

The ICO says exemptions should not be routinely relied upon or applied in a blanket fashion. You'll need to demonstrate how an exemption applies and your rationale for relying on it. It's possible you may need to provide evidence of this to the ICO or the courts.

Commonly use exemptions

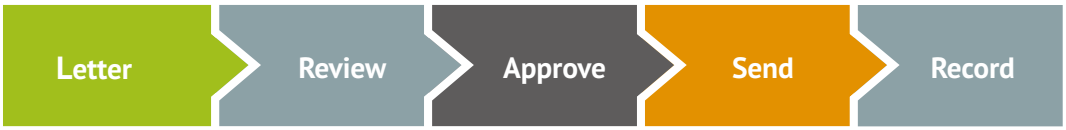
- Legal professional privilege
- Management information
- Negotiations with the requester
- Journalism, academia, art & literature
- Confidential references
- Crime and taxation
- Research and statistics
- Health, education and social work
- Exam scripts and exam marks

The full list of exemptions can be found in Schedule 2, Data Protection Act 2018. Examples of how they apply can be found in the *ICO's right of access guidance*.

> *While it is essential to respond to DSARs, it is vitally important to know what the limits are on DSAR requests and have appropriate escalations, so you can ensure you do not allow yourself to become a source of data breach, or disclose commercial or sensitive security information.*
> **Ray Pathak, Vice President Data Privacy, Exterro**

8. Final steps

Once the personal data has been retrieved, collated and redactions (or exclusions) have been applied, there are a few final steps to cover off before the response can be sent and the request closed.



8.1 Covering letter

It can save time to have at least one standard template covering letter, which can be adapted as necessary depending on the nature of the request.

Covering letter contents

- ✓ Describe personal data being provided
- ✓ Explain internal terminology or other uncommon terms
- ✓ Include supplementary information, (or link to Privacy Notice - if all covered)
- ✓ Explain use of redactions

8.2 Review and approve

You'll need to make sure it's clear who, or which team, is responsible for reviewing and approving the final response before it's sent. This should be someone (or people) with sufficient knowledge of the process and the requirements, and a suitable level of seniority.

8.3 Send securely

Responses must be sent securely in a 'structured, commonly used and machine-readable format'. Generally if someone has submitted their request electronically, you can respond with an electronic copy of their personal data.

It should be easy for the individual to access the response. You shouldn't force people to download a particular app or programme in order to access their data. If someone would prefer you to send the documents by post, this should be considered unless unreasonable.

> *When responding to a request by email, the information must be sent securely. Often (depending on the secure email solution) the secure email will look different from the regular email address that the DSAR was sent to and/or acknowledged from. It is advisable to follow up immediately with an email (from the regular email) to ask the recipient to confirm that they have received the information and are able to view it. Their reply will serve as proof of receipt of the response. If your secure email solution can track when the response was viewed and the information downloaded, save this receipt with the DSAR records.* **Temi Akindele | Data Protection & Legal Counsel | The Prince's Trust**

8.4 Record keeping

Crucially, we need to keep records of DSAR requests and not just when they were received and when we responded.

DSAR closure checklist

- ✓ Close the request on DSAR log
- ✓ Record response date
- ✓ Keep a record of the response
- ✓ Keep a record of decisions taken and justifications for exemptions
- ✓ Retain a copy of the response
- ✓ Agree a suitable retention period

9. How technology can help

Organisations need to log requests, keep records, effectively retrieve information, manage workflows, review documents, apply redactions where necessary, and respond on time.

This can all be done using routine business tools. However, where DSARs are becoming unduly time-consuming and costly, technical solutions can help to automate and streamline the process. These might be developed in-house, or via an external provider.

Technology solutions can significantly reduce the time taken and costs involved in handling DSARs.

9.1 Why use a technology solution?

It's worth analysing how much it actually costs you on average to fulfil a DSAR. Plus assessing any risks you may be exposed to, for example by failing to respond in time or errors being made under pressure. Even if you keep an eye on the working hours they take to fulfil, losses incurred by diverting resources can often be overlooked.

What risks are you potentially exposed to?

- Failure to validate identity could lead to a data breach.
- Ineffective searches will result in incomplete responses.
- Time pressures can increase the likelihood of mistakes.
- A lack of sufficient records can mean an inability to respond to complaints.
- An inefficient process raises the likelihood of complaints and regulatory scrutiny.

9.2 What technology solutions are there?

There are a wide range of external solutions which vary in cost and sophistication. Some are AI-driven, others aren't. Some support the end-to-end process, others help to streamline specific elements such as identity verification, data discovery, data analysis, document review and redaction.

There will be a decision to be made about whether to implement a system which covers the whole process, or whether there are certain tasks you'd like to focus on to achieve efficiencies.

The above is not an exhaustive list but provides an illustration of the types of areas technology solutions can help streamline the process, reduce the time requests take and the lower the costs involved.

What can tech do?

Request portals
Requests can be submitted by your own dedicated portal. Which may also provide automated identity verification.

Data discovery / automated searches
Integration with your systems to allow for efficient automated searches.

Data analysis
Advanced searching functionality can enable the review of data from all connected systems "in place" without having to copy or touch the data first. Providing quick upfront insight.

Workflow management
Helping people across the organisation collaborate on locating the data and responding within the required timeframe.

Auto-assigning tasks
Ensuring relevant stakeholders are notified when they have an action to undertake.

Maintaining logs
Keeping records of all requests, their status and other information.

Reducing data volume
Identifying and removing irrelevant items from retrieved data.

Document review
Technology can help staff, external counsel, or both to manage the review process reducing time and cost in what's typically the most time-consuming and expensive part of handling a DSAR.

Redaction
Tools can support the application of redactions. A time and cost-saving solution if you're currently undertaking manual redactions.

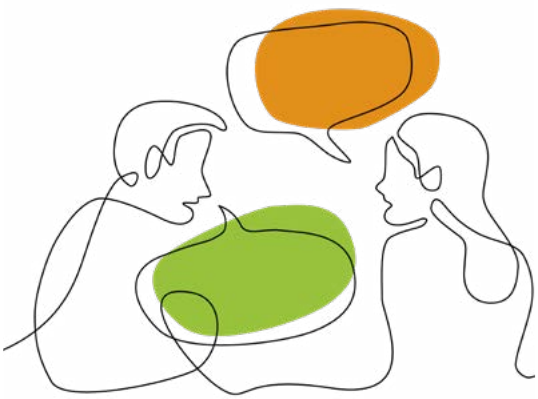
Document production
Some tools can prepare the documentation and securely send the response.

The above is not an exhaustive list but provides examples of where technology solutions can help streamline the process, save cost and time.

About DPN

Data Protection Network (DPN) publishes expert analysis, insight and resources. Our content is written and developed by a team of data protection specialists, members of our Advisory Group and other respected contributors.

In 2017 the DPN published the first definitive industry guidance on legitimate interests and in 2020 we published detailed data retention guidance. In 2022, the DPN has published its inaugural Privacy Pulse Report to test the temperature of the data protection and privacy community.



The DPN also runs regular webinars where DPOs and other privacy professionals share their experiences and practical tips.

How we can help

Our experienced team provide no-nonsense privacy advice and support, across a range of sectors. Our goal is to make data protection relevant and easy to understand. Based on extensive real-world experience, our team continues to stay at the forefront of data protection. To learn more about us visit: *dpnetwork.org.uk*.

exterro

About Exterro

Exterro empowers the world's largest organisations, law firms and Government agencies to proactively and defensibly manage their Legal Governance, Risk and Compliance (Legal GRC) requirements.

Exterro's Legal GRC software is the only comprehensive platform that automates the complex interconnections of data privacy, legal operations, digital forensics, and cybersecurity compliance. Thousands of legal teams, IT leaders and investigators around the world trust our integrated Legal GRC platform to manage their risks and drive successful outcomes at a lower cost. For more information, visit *www.exterro.com*.

Exterro Privacy Software

Quickly and easily identify, map, manage and protect your organisation's data to establish robust global privacy compliance processes.

Exterro provides the most effective and defensible way to accurately develop and maintain a comprehensive data inventory. Combined with the ability to efficiently leverage data and records retention rules that address legal and business requirements while reducing risks and costs, you'll be in safe hands with the world's most trusted software solutions for meeting domestic and international regulatory obligations.

www.dpnetwork.org.uk

DATA PROTECTION NETWORK