

Navigating the DSAR Minefield

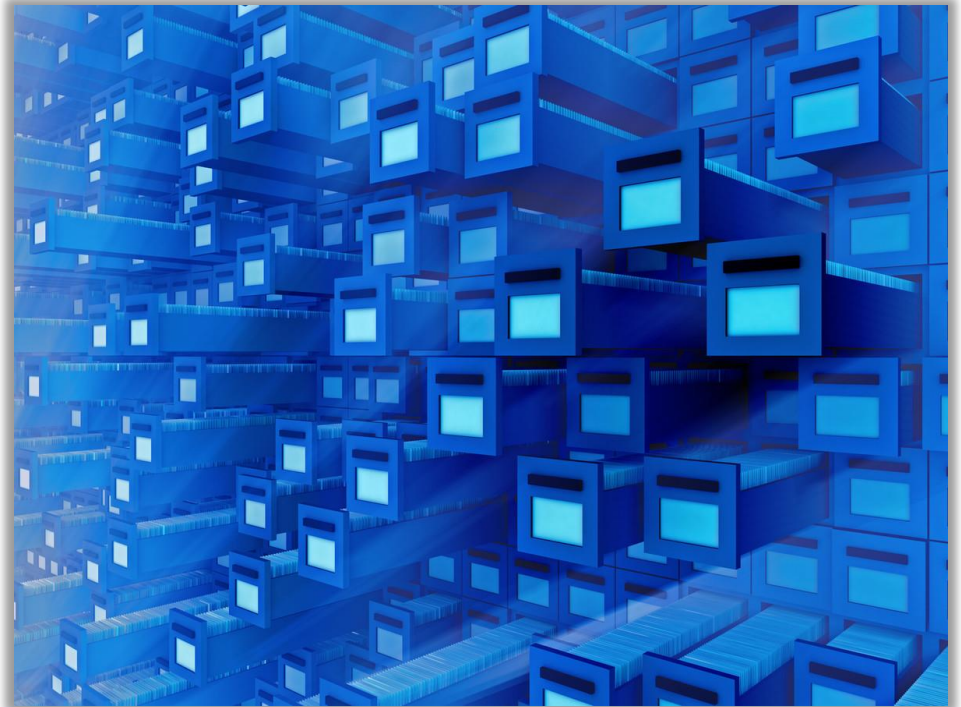
3 December 2019

(as amended to reflect the changes made to the 'right of access' section of the ICO's GDPR guidance made after this presentation was created and delivered)

By Francesca Fellowes and Emma Yaltaghian

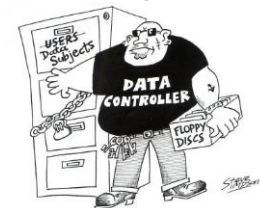


- What is a DSAR?
- Introducing our Case Study
- Initial considerations – Q&A
- First steps
- Locating the data
- The review – third party data and exemptions
- Practical examples
- The response



What is a Data Subject Access Request?

- Right of access under Article 15 of the GDPR: The right to receive:
 - Confirmation of whether their personal data is processed
 - A copy of their data
 - Supplementary information
 - To understand how and why data is processed about them, and check the use is lawful
 - One calendar month to respond in most cases
 - Can request proof of ID where there is 'reasonable doubt' as to the identity of the requestor
 - Usually no fee



Introducing our Case Study: Part I

You are an HR Manager and when you arrive in the office on 20 December 2019, you open up your emails to find the below request.

To:	HR
From:	samdawson@icloud.com
Subject:	Data Subject Access Request
Date:	20 December 2019

I am writing to request access to all my personal data.

I would like you to respond to my request within one month, failing which I will be forwarding my request together with a letter of complaint to the Information Commissioner's Office.

I also require sight of my personnel file.

Sam Dawson

Introducing our Case Study: Part II

- Sam has worked with the company as a Customer Services Representative since 2014.
- In September 2019 he raised a grievance, which you recently responded to – the grievance was not upheld.
- The DSAR may be an attempt to locate evidence to use in support of an appeal or action against the company.
- You notice that the request has not come from Sam's work email address. Sam and the Company are UK based.



Is it a valid data subject access request? ✓

- Yes: Any request by an individual for their own personal data – verbal or written. Does not need to refer to Article 15 or ‘subject access request.’
- Can be submitted to any part of the company, including by social media – raise awareness.
- Can encourage, but not require use of standard form.

Motive? X

- Does it make any difference that you suspect Sam is on a “fishing expedition” to try to obtain information to support a possible employment tribunal claim or grievance appeal?
- No - motive is usually irrelevant.

Can we charge a fee? X

- Usually no, except a “reasonable fee” for the administrative costs if the request is:
 - manifestly unfounded or excessive (see below); or
 - it is a request for further copies of data.

When can we refuse to comply with a request?

- When certain specific exemptions apply under the DPA 2018; or
- If the request is:
 - manifestly unfounded; or
 - excessive.

Must be able demonstrate this to the ICO



ICO guidance:

Request may be manifestly unfounded if:

- The individual clearly has no intention to exercise their right of access. For example an individual makes a request, but then offers to withdraw it in return for some form of benefit from the organisation; or
- The request is malicious in intent and is being used to harass an organisation with no real purposes other than to cause disruption. For example:
 - the individual has explicitly stated, in the request itself or in other communications, that they intend to cause disruption;
 - the request makes unsubstantiated accusations against you or specific employees;
 - the individual is targeting a particular employee against whom they have some personal grudge; or
 - the individual systematically sends different requests to you as part of a campaign, e.g. once a week, with the intention of causing disruption.

Not a simple tick box exercise – consider the context.
Genuine intention to exercise their rights?

Request may be excessive if:

- it repeats the substance of previous requests and a reasonable interval has not elapsed; or
- it overlaps with other requests.
- It will **not necessarily** be excessive just because the individual:
 - requested a large amount of information - consider asking the data subject for more information to help you locate their data (see below);
 - wanted to receive a further copy of information they have requested previously. You can charge a reasonable fee, but not likely to be excessive;
 - made an overlapping request relating to a completely separate set of information; or
 - previously submitted requests which have been manifestly unfounded or excessive.

- When deciding whether a reasonable interval has elapsed you should consider:
 - how frequently the data is altered – is it likely to have changed between requests?
- If you decide to refuse a request you must inform the requestor without undue delay and within one month of receipt of the request about:
 - the reasons you are not taking action;
 - their right to make a complaint to the ICO or another supervisory authority; and
 - their ability to seek to enforce this right through a judicial remedy.
- You should also provide this information if you request a reasonable fee or need additional information to identify the individual.

Should we request proof of ID?

- If there are doubts over the identity of the data subject. Request proof of ID/fee promptly.

Case Study

- You checked and the requestor's personal email address matched the address on file and so no proof was needed.

How long do we have to respond?

- Without undue delay – up to 1 calendar month from the date of receipt of the request.

Case Study

- Request received by email on 20 December 2019. Deadline is 20 January 2020. Xmas holidays do not stop the clock!
- If the response date falls on a weekend or bank holiday, the deadline moves to the next working day.
- If the following month is too short, so no corresponding date, the deadline is the last day of the month ie. Request: 31 March, respond 30 April.

When can we extend the deadline?

- The deadline can be extended by a further two months if the request is:
 - Complex; or
 - You have received a number of requests from the individual
- No guidance on meaning of ‘complex’ but likely to be something over and above the ordinary. (NB: ***Some clarification is now provided in the ICO’s new draft guidance published after these slides were created***)

Case Study

- Nothing here to suggest that the deadline can be extended.
- If you ask for ID/a fee (promptly), the clock does not start to run until you get it.

WARNING: Since these slides were created, the ICO has amended its guidance to state that the time limit for a response is **NOT** paused whilst you wait for the additional information to locate the data.

Log the request – name of requestor, date received, scope of request and deadline for a response

Identify and alert all key stakeholders: HR, IT, DPO, legal etc

Start the searches – IT to search relevant systems/mailboxes

Locate and start to review Personnel File

Initiate a ‘document hold’ so that files are not accidentally deleted

Acknowledgement letter to requestor

- Take steps to locate requester's data in filing and electronic systems. Can also be in time recording systems, CCTV etc.
- ICO subject access code of practice: *"Given that subject access has been a feature of data protection law since the 1980s, your information management systems should facilitate dealing with SARs"*.
- Use name/variations, initials, nicknames, other identifiers, such as employee number to run an initial search for his data.

Case Study

- Initial searches reveal 40,000 documents/emails.
- Disproportionate to third party privacy to manually review a large volume of documents/emails?

Case Study

- You decide that you need more information to locate Sam's personal data. You email him on 27 December asking for date ranges, subject matter, mailboxes.

Recital 63:

“Where the controller processes a large quantity of information concerning the data subject, the controller should be able to request that, before the information is delivered, the data subject specify the information or processing activities to which the request relates.”

■ ICO

- You can only ask for information that you reasonably need to find the data. Make the request promptly. (**NB:** this wording in the ICO’s amended GDPR guidance has now changed)
- If the individual refuses to provide additional information *“you must still endeavour to comply with their request ie by making reasonable searches for the information...”*

■ Case Study

- Sam responds on the same day to say that he wants data relating to his grievance.
- Deadline – Now runs from 27 December – 27 January. **WARNING** – This is no longer correct according to the ICO’s new guidance published after these slides were created. The deadline would remain 20 January.

■ Case Study

- You take steps to manage the 40,000 initial hits by:
 - Applying a suitable date range: the circumstances relevant to the grievance occurred from June 2018.
 - Applying search terms relevant to the grievance.
 - Limiting the mailboxes searched.
 - Removing 'false positives' ie. Samantha and duplicates.
- Documents reduced to 3,000.

■ Next steps

- Manually review:
 - To locate Sam's personal data.
 - To remove/make decisions about third party personal data.
 - To apply exemptions.

Identify Sam's personal data – any information which relates to him. Can it be used to 'learn, record or decide' something about him?

Remove/redact third party personal data and information relating solely to the company.

He is not entitled to information relating to other people, unless it is also about him.

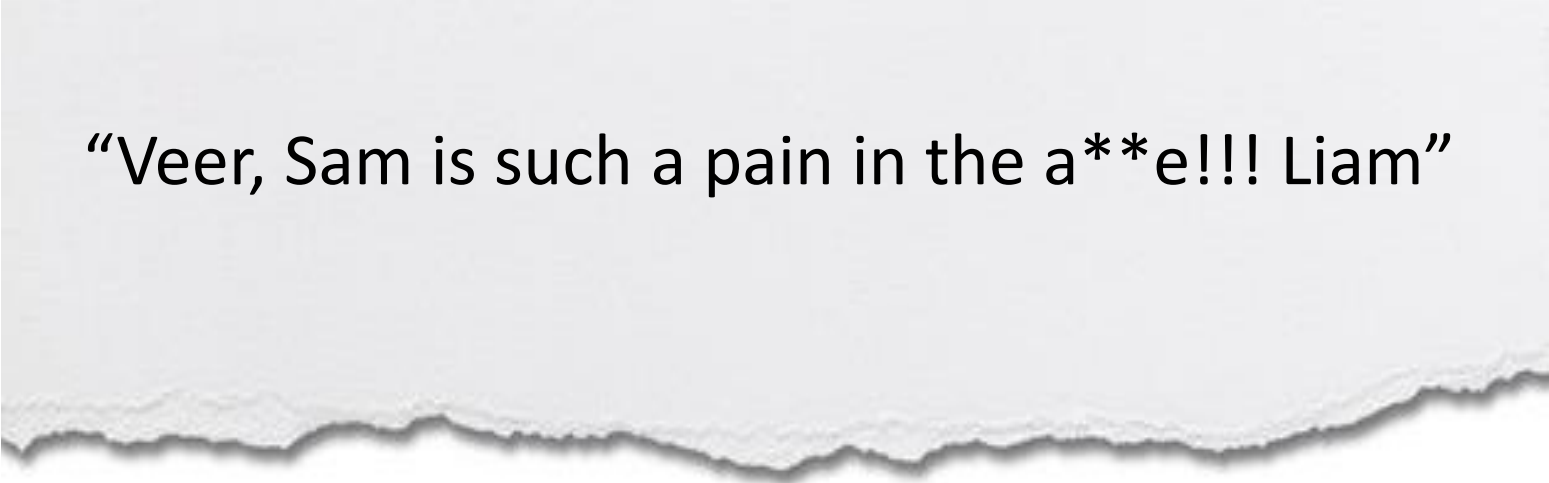
He is entitled to the data NOT the document

CCTV - print stills and blank out other individuals

- The DPA 2018 says does not oblige a controller to disclose information to the data subject to the extent that doing so would involve disclosing information relating to another identifiable individual, except if:
 - the other individual has consented to the disclosure; or
 - it is reasonable to comply with the request without that individual's consent.
- In determining whether it is reasonable to disclose the information without consent, you must take into account all of the relevant circumstances, including:
 - the type of information that you would disclose;
 - any duty of confidentiality you owe to the other individual;
 - any steps you have taken to seek consent from the other individual;
 - whether the other individual is capable of giving consent; and
 - any express refusal of consent by the other individual.

It is a balancing exercise between the importance to the requestor to get the information and the prejudice to the third party if it is disclosed

Email from Liam to Veer (employees managed by Sam) in relation to Sam



“Veer, Sam is such a pain in the a**e!!! Liam”

Email from Indy (Sam's colleague) to HR

“Lauren and Chloe were saying that Sam is not good enough to get a pay rise, he is lazy and doesn't do enough work.

Chloe said that she deserved a pay rise instead.

I don't think they should be discussing their colleague in the open plan!”

Limited exemptions

Negotiations with data subject

“personal data that consists of records of the intentions of the controller in relation to any negotiations with the data subject to the extent that the application of those provisions would be likely to prejudice those negotiations”.

Management Forecasting

“processed for the purposes of management forecasting or management planning...to the extent that the application of those provisions would be likely to prejudice the conduct of the business or activity...”.

Privilege

claim to legal professional privilege; or
“duty of confidentiality is owed by a professional legal adviser to a client of the adviser”.

Confidential references

“a reference given (or to be given) in confidence” for the purposes of education training or employment, volunteer placements, office appointments or service provision. Applies to the provider of the reference and the recipient.

Email from Helen to Nathan (copying in Emily, the Company's external legal adviser)

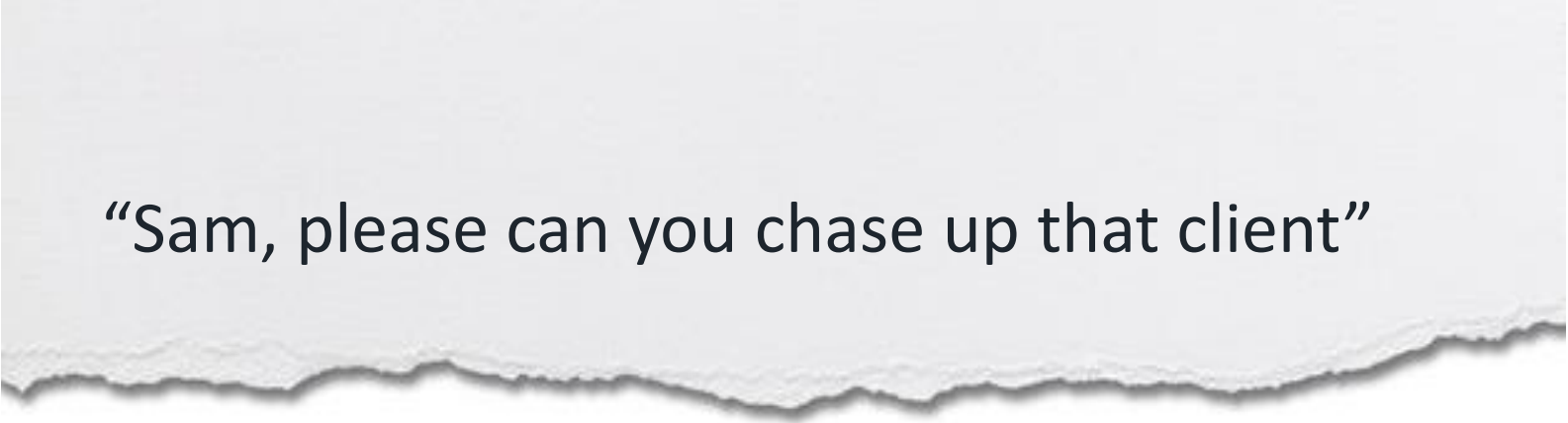


“Have cc'd Emily for privilege”.

Email from Emily (Company's external legal advisor) to Helen in relation to Sam's grievance

“As discussed, I have been through Sam's grievance and I have the following comments to make...
Yours, Emily.”

Email from Nathan to Sam



“Sam, please can you chase up that client”

Collate a final pack of documents

Careful quality check: read the documents from the perspective of the requester/their adviser – any gaps ie. attachments to emails, other emails in the chain?

Do they have everything they have requested? If not, provide explanation in the covering letter.

GDPR: provide data electronically if the request has been made electronically, unless requested otherwise. Secure method ie. encrypt or track if sending by mail.

Recital 63: Ideally provide remote access to a secure self-service system.

Response letter: covering letter must include all 'supplementary information' listed in Article 15. Clear and intelligible to that particular individual. Consider audience. De-code where necessary.

The Response: covering letter

- The purposes of your processing;
- The categories of personal data concerned;
- The recipients or categories of recipient you disclose the personal data to;
- Your retention period for storing the personal data or, where this is not possible, your criteria for determining how long you will store it.



The Response: covering letter

- The existence of their right to request rectification, erasure or restriction or to object to such processing;
- The right to lodge a complaint with the ICO or another supervisory authority;
- Information about the source of the data, where it was not obtained directly from the individual;
- The existence of automated decision-making (including profiling); and
- The safeguards you provide if you transfer personal data to a third country or international organisation. This information may be contained in a privacy notice.



Top tips for responding to DSARs

Top Tip 1

Notify key stakeholders and start the searches as soon as you get the DSAR

Top Tip 2

Communicate with the data subject – provide what you can when you can, if late

Top Tip 3

Proof read the pack of documents from the data subject's perspective

Top Tip 4

Keep a clear record of what you have (and have not) disclosed

Top Tip 5

Don't panic!

Today's presenters



Fran Fellowes

Director, Leeds
Data Privacy & Cybersecurity
T: +44 113 284 7459
E: francesca.fellowes@squirepb.com



Emma Yaltaghian

Associate, London
Data Privacy & Cybersecurity
T: +44 020 7655 1515
E: emma.yaltaghian@squirepb.com