



Dealing with Data Subject Access Requests

Wed 7 Sept 2022

In today's Breakfast Briefing



Dealing with DSARs

- > Legal background of DSAR
- > Explanation of personal data
- > Top tips when dealing with a request
- > Communicating sensibly in context of DSARs
- > Useful resources



The law on DSARs



Legal context of DSARs



- > Under the UK GDPR a data subject may make a subject access request and a controller is under a duty to comply. In this note, "employer" refers to the controller and "employee" to the data subject (who may be an employee, worker or other type of staff).
- > Data protection in the UK is governed by the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) (UK GDPR) and the Data Protection Act 2018 (DPA 2018)
- > Information Commissioner's Office (ICO) published detailed guidance on the right of access

What is personal data?



- > Article 4(1) of the UK GDPR defines as:

"'Personal data' means any information relating to an identified or identifiable living individual ('data subject')."

- > Name, ID number, location data, online identifier to one or more factors specific to the characteristics of that person (physical, mental, economic, or social characteristics)
- > Employment context: emails about individual, payroll information, occupational health reports, meeting minutes etc
- > Some personal data is in a 'special category' which needs more protection. There are specific conditions for processing this type of data and data protection impact assessment is usually required.
- > Special category: race; ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; genetic data; biometric data (where this is used for identification purposes); health data; sex life; or sexual orientation.



How to deal with requests



- > Top tips to help guide you through the whole process

Responding to requests



- > Can be time consuming and heavy on resources
- > Often linked with ongoing dispute or litigation
- > Three broad rules when responding as per UK GDPR:
 - The employer must facilitate the exercise of the subject access right, *Article 12(2)*
 - The request must be handled lawfully, fairly and transparently, *Article 5(1)(a)*
 - Information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language, *Article 12(1)*
- > 1 month to respond to the request – may be extended by 2 months depending on complexity and number of requests at any one time. Must inform employee within one month of any delay with reasons

Responding to requests

Initial Assessment



- > Give the request an initial assessment to refine process for efficiency – always acknowledge the request
- > **Verify the identity of the individual requesting the personal data**
 - May be no need to verify identity e.g. ongoing relationship
 - Keep simple e.g. utility bill or copy of driving license
 - Don't pause whilst identification process goes on – start preparing for your search!
- > **Clarify the request and communicate with the requestor at this initial stage**
 - Ask for clarity on their request – usually will narrow scope down if you make it clear the purpose is to give relevant and pertinent information
 - Specific time period, relevant to a certain event, particular category of data?
- > **Preparing your search criteria**
 - Consider what you are searching for – how do you reference people?
 - Where – multiple inboxes/ back up drives/ archive
 - Strategy – may be hundreds of thousands with solely a name e.g. emails sent to them, which they are not subject of

Responding to requests

Form of response



- > The legal right is to receive a copy of the data, not original documents
- > The format of how to deliver all the information obtained through search is discretionary and dependent on available resources/ time/ software the company has
- > Consider which method will provide the information in the most accessible and clear way when determining
- > Redaction method
 - Provide screenshots/ scans of original document (e.g. email) with redactions of any personal data of another individual
 - Need appropriate tools e.g. Adobe, or outsource
 - Level of redaction depends on approach – no requirement to supply information that is not personal, but cheaper to leave in
- > Extraction method
 - Extract personal data from original location and paste onto a clean separate document e.g. excel spreadsheet, report
 - Allocate date, time and put information regarding the personal data – provides document which can be easily navigated
 - May be useful when there is a large quantity of repetitive data

Responding to requests

Exemptions



- > Legal advice or litigation privilege
- > A reference given, or to be given, in confidence for employment, training or educational purposes
- > personal data which is processed for the purpose of management forecasting or planning for business activities where disclosure would prejudice the business activity, e.g. disclosing information on a staff redundancy programme before it has been announced to the affected workforce. Redundancy exercises relating to the individual which have been concluded are not likely to fall within this exemption.
- > Employers also do not have to disclose records relating to negotiations between the employer and employee, if to do so would prejudice those negotiations

FAQ to our team



- > What if the data discloses information which identifies another individual?
 - Information Commissioner approach that ideal approach is they would consent to their data being disclosed but this is not always possible or appropriate, and there is no requirement or legal obligation to do so either
 - Balancing exercise between individual making request and third parties competing rights
 - This third-party information can be redacted to give the requestor as much of what they are seeking but protect data of individuals

- > Do I need to respond?
 - If a request is 'manifestly unfounded or excessive' the employer may decide not to respond but must give reasons to the employee and advise they can complain to the Information Commission or apply to court
 - Extremely high risk deciding not to respond on this basis as ICO have expressed they will look closely at reasons – high threshold
 - Take advice before making this decision – may be more appropriate to clarify the request to narrow scope and respond to the extent you find proportionate

- > The employee making the request is only copied into this email, do I need to include?
 - If they are not the data subject of the email but simply on a recipient list (e.g. meeting invite or general employee information) then no obligation to disclose this data
 - Again depends on approach of employer to the search

Communicating safely



- > General rule of thumb: if you wouldn't feel comfortable with it being read out in a tribunal or court – don't put it on an email!
- > Raise awareness in team of data protection implications – IT Communications/ Data protection policies & training
- > Don't mix personal conversations in emails relating to work matters
- > Before sending communication consider whether any personal data **needs** to be disclosed
- > ICO guidance on use of personal email addresses / social media platforms for work capacity – may fall under scope of request

Useful resources



- > [Right of access/subject access requests and other rights | ICO](#)
- > [How to deal with a request for information: a step-by-step guide | ICO](#)



Thank you



scoteng.org.uk | 0141 221 3181