

Footnotes To Do's and Don'ts of Employee or Customers DSARS in the UK

1. Sources : [UK GDPR](#) ; [Data Protection Act 2018](#) for specific details and exemptions; [Part 5 Data \(Use and Access\) Act 2025](#); [ICO DSAR](#) , [ICO DSAR sources](#); [Subject Access Request Q and As For Employers](#); podcasts such as [Privacy Unpacked Episode 3: Mastering DSARS: Employment Conversations Data Subject Access Requests \(DSARS\) and how employees should respond](#); [HR Data Essentials: Breakout session 3: DSARs: latest cases and practical compliance](#).
2. [art 4\(1\) UKGDPR](#) ; [ICO](#) ; [Rec 26 UK GDPR](#); (i) What qualifies as personal data see *Durant v Financial Services Authority* [2003] EWCA Civ 1746; *Edem v Information Commissioner & Financial Services Authority* [2014] EWCA Civ 92; (ii) Extent of search see *Dawson-Damer v Taylor Wessing LLP* [2017] EWCA Civ 74; *Deer v University of Oxford* [2017] EWCA Civ 121; *DB v General Medical Council* [2018] EWCA Civ 1497; (iii) form of disclosure see *Itihadieh v Etihad Airways / Deer v University of Oxford* [2017] EWCA Civ 120 (Joint Appeals).
3. A DSAR is a right to request confirmation of whether you are holding or using their information and other supplementary information. It is a right to obtain a copy of your personal data, not carte blanche to receive full documents. There are no formal requirements for making a DSAR; they can be oral or in writing and submitted to anyone in the organisation. They can be email-requests generated by platforms or even requests made on social media. [Art15 UK GDPR](#)
4. Useful digital solutions include platforms such as OneTrust and DataGrail and mor users of M365, software called Microsoft Purview eDiscovery. The cost of using eDiscovery, in the case of 500 plus documents, is likely to prove may cheaper as compared to the human cost of review.
5. This will enable you to create fields to help understand the nature of request, manage time constraints and record your responses. OneTrust Platforms offer such capability. Typically, you would invite data subjects to access the form via a hyperlink in your privacy notice.
6. This works well if the DSARS are process driven and the level of data held about individuals is low. It's much more challenging if the data held on an individual is complex e.g. in the case of employee DSARS when an individual is going through a grievance, disciplinary proceeding, has been sacked, being made redundant or from an unsuccessful applicant.
7. Without undue delay means within one month unless there are grounds for extension. The clock starts ticking when the request is made but may be paused (i) on the day you request clarification and resume on the day you receive it; (ii) on the day you request ID documents and resume on the date of verification. [art 12A UK GDPR](#); [\[Rec 59 UK GDPR](#); [DPA s45\(3\)](#); [DPA s54\(2\)\]](#)
8. If an individual submits a DSAR electronically (e.g., via email, web form, or social media), the controller must provide the response in a commonly used electronic format (such as PDF or secure email export), unless the individual specifically requests another format. [Art 15 \(3\) UKGDPR](#)
9. *Examples of invalid requests.* (i) request on behalf of another without signed letter of authority/ power of attorney, (ii), request from a generic email address owned by a platform requiring payment of a fee/ to sign up to a service to see the DSAR (iii) third party portal has not provided evidence it is acting on behalf of a data subject and that data subject has agreed to uploading the info to the portal; (iv) certain requests from children.

Examples of valid requests. (i) requests sent from individuals email accounts (who have signed up to a service such as Mine or Privacy Hawk that grant access to their inbox to scans it to see which companies have communicated with the individual to see who is likely processing personal data about that individual) by a service are valid; (ii) requests for data from WhatsApp messages or similar are valid if you are directing staff as an employer to use third party tools or are at least aware of or not condoning such use for work purposes. This would be considered under your control.
10. If you have any doubts about the requester's identity, it's reasonable to ask them to verify their identity before sending the information. [Art12\(2\) UK GDPR](#); [12A\(5\) UK GDPR](#); [\[S52\(4\) DPA\]](#)
11. You can (i) clarify if the request is vague or you hold a lot of information about the individual e.g. to help you identify the personal information or the processing activity that the SAR relates to. However, you should not ask for clarification on a blanket basis. You cannot force an individual to narrow the scope of their request, as they are entitled to ask for all their information; or you can (ii) not seek clarification, and you choose to perform a reasonable search instead. [UK GDPR art 12A\(6\)](#); [ICO](#)
12. Data subject are entitled to the following supplementary information: (i) purpose of processing; (ii) the categories of the personal data concerned; (iii) who is receiving the personal data; (iv) how long the personal data will be retained; (v) the existence of the right of the data subject to request rectification/ rectification/ erasure of the personal data or restrict its processing in certain circumstances; (vi) right to lodge a complaint with the ICO; (vii) if the data has not come from the data subject themselves then where that data came from; (viii) if there is any automated decision-making including profiling. If supplementary information is satisfactorily covered by a privacy notice you can simply provide a copy or link to it. Be on the lookout for potentials hurdles relating to matter such *any recipients or categories of recipients to whom the data has been disclosed and the retention period for the data*. Note, UK revisions to the UK GDPR have

adopted some EU case law but not all e.g. it has not adopted the findings in EU CJEU's *UI v Österreichische Post AG* read with *AG Pankow* which means that the name of employees, who have seen the personal data, may need to be disclosed. [UKGDPR art 15\(1\); \[S 45\(2\) DPA\]](#); [ICO](#)

13. This includes information stored by your processor or information stored by staff on their personal device about customers, contacts or other employees. For employee DSARS main sources of data are typically company specific emails and other forms of communication such as chatbots, instant messages; HR systems such as payroll, HRIS systems for employees; and customer data bases when dealing with consumers. [ICO](#)
14. Agree who's responsible for retrieving the data, reviewing the data, applying exemptions, applying redactions/ extracting data, reviewing the response, approving it and sending it out securely.
15. This is the most important stage to determine the volume of data and resources needed to review it.
16. The obligation to search is not absolute; you are not expected to leave "no stone unturned." *Dawson-Damer v Taylor Wessing LLP* [2017] EWCA Civ 74. The court considers the burden, cost, and complexity of retrieving data versus its value to the data subject. You may comply with your obligations even if you have not found every item within the scope of the request i.e. your search could be limited to the employee's full name and unique employee ID excluding a blanket search for common initials on the grounds that that is disproportionate and likely to return vast amounts of third-party data. This is consistent with ICO guidance which emphasises that proportionality is relevant consideration as distinct from EDPB guidance and EU GDPR which does not. [Art 15 \(1A\) UK GDPR](#); [ICO](#)
17. A further two months, [art 12A UK GDPR](#); [\[S 54\(3A\) DPA\]](#).
18. [ICO](#) A request may be complex if it is more than one request i.e. spans multiple channels such as emails, WhatsApp, Teams etc; likely to return vast amounts of third-party data; held in multiple locations (e.g. employee has worked in different departments/ for different subsidiaries, in different countries). It will depend on the tools at your disposal. It is not uncommon to rely on extensions for employee DSARS.
19. Send a complexity extension notice to the individual, extending response window by a further two months. [art 12A\(3\) and 12A\(4\) UK GDPR](#); [\[S 54\(3B\) DPA\]](#)
20. [Art12\(5\) UK GDPR](#); [\[S 53 DPA\]](#)
21. *Manifestly unfounded*. Employee has no real intention of exercising their right of access (e.g. the employee makes it clear they will withdraw their request in exchange for some form of benefit); or the request has been made maliciously to harass the employer (e.g. employee makes multiple wide reaching requests which are clearly intended to disrupt the business (i.e. have said that they want to make the employer pay) or made it clear that request is part of a personal grudge (i.e. have made unsubstantiated allegations against a particular employee)). Note fishing requests / pre action disclosure requests are valid. [ICO](#)
22. *Manifestly excessive*. Clearly and obviously unreasonable considering the burden and costs involved in dealing with the request e.g. where a data subject has made multiple overlapping requests during a continuous period. Comes down to facts i.e. employers' resources and whether a previous request for the same information has been made. [ICO](#)
23. [Art12\(5\) UK GDPR](#); [\[S53\(3\) DPA\]](#)
24. This will enable you to (i) refine data; (ii) de-duplicate data; (iii) thread in conversations to keep things together; (iv) navigate between documents; (v) jump to where the key words appear; (vi) flag documents that (a) can be disclosed in full, (b) which contain no data, (c) which contain data that needs to be extracted or redacted, (d) privileged documents, (e) documents that fall outside scope. Once flagged the documents can be pulled into documents sets, that can be disclosed.
25. See "Don't" below. The individual making the request is not entitled to information which contains personal data of another individual unless (i) the other individual has given consent to the disclosure or (ii) it would be reasonable to comply without the individual's consent. The latter exception involves balancing the requestors rights vs another individual's privacy. Factors to consider include: the type of information, whether there is any duty of confidentiality, whether any attempts have been made to obtain consent from the other individual. [DPA Sch Part 4 Para 16](#); [ICO](#)
26. See "Don't" below. Exemptions include legal advice/ litigation, management restructuring, settlement negotiations, third party identities, confidential references, internal criminal investigations. [ICO](#)
27. You must clearly explain why the data or request is being refused or redacted or identifying a specific statutory exemption (see notes below), such as Legal Professional Privilege or Third-Party Rights). If the ICO later investigates a complaint, the burden of proof rests on the organisation to demonstrate why the refusal or redaction was lawful. 5(2) and [12\(4\) UK GDPR](#); [\[DPA 45A\(4\)\]](#)
28. The pre GDPR case in the UK of *Durant v Financial Services Authority* [2003] EWCA Civ 1746 states that data subjects are entitled to data, not documents. To qualify as personal data, information must satisfy two main criteria: (i) it must

be biographical in a significant sense (going beyond a minor record of an event or transaction), (ii) it must have the individual as its focus rather than another individual, transaction, or corporate investigation.

29. For example in the case of an employee DRSAR recruitment and onboarding documents (i.e. job application and CV, interview notes, vetting and security checks, offer letter and contract) Personnel HR & Administrative records (i.e. personal file extracts, attendance and attendance logs, training records), Payroll compensation and benefit records (i.e. pay statements, salary and bonus letters, benefits documentation), employee relations and investigations and disputes (i.e. grievance records, disciplinary records) health, safety and welfare records, Access, security and CCTV records (i.e. building swipe logs, CCTV extracts, IT audit/login logs)
30. GDPR does not prescribe a set format for providing the data, although there is a recital at the beginning of GDPR which says that where possible organisations should be able to provide remote access to a secure system which would provide data subjects with direct access to their personal data. If that is not possible then provide it in a csv file. [ICO](#)
31. A breach is considered a significant breach and could lead to a fine of £17,5 million or 4% of world-wide turnover whichever is the greater figure. An individual can sue for compensation provided they can show that they suffered damage or distress as a result.
32. In the UK it is a criminal offence to prevent disclosure of data that ought to be disclosed under a DSAR, unless you can show reasonable belief that this could be withheld.
33. See footnote 25 above. [DPA Sch Part 4 Para 16](#)
34. You will be disclosing the fact that the requestor has made a DSAR
35. See footnote 11 above.
36. This exemption covers the two branches of legal professional privilege: litigation privilege and legal advice privilege. [DPA Sch Part 4 Para 19](#); [ICO](#)
37. [DPA Sch Part 4 Para 20](#); [ICO](#)
38. You are not required to provide certain internal management discussions relating to management forecasting and planning (like premature disclosure of HR's strategy for the disciplinary hearing, emails discussing the strategy, timing, or potential outcomes of the disciplinary process), so long as can prove *disclosing them would prejudice the business's ability to manage its workforce*. [DPA Sch Part 4 Para 22](#); [ICO](#)
39. Personal information that is a record of your intentions in negotiations with a person is exempt from the right of access. This only applies to the extent that complying with a DSAR would likely prejudice the negotiations. [DPA Sch Part 4 Para 23](#); [ICO](#)