Practical Insights for Responding to Employee DSARs - A Primer

PROSEARCH WHITE PAPER SERIES

PROSEARCH
LOVE WHAT YOU DISCOVER

Summary

Responding to data subject access requests (DSARs) from employees or ex-employees can be a significant challenge. Required response times remain unchanged, though the volume of electronically stored information within the scope of a request can be extensive. Sufficient preparedness and reliable methods for narrowing large datasets down to specific, granular disclosures of a requestor's personal information can save organizations time and expense, while keeping regulators at bay.

> The data subject access request, or DSAR, is the most widely exercised individual right afforded by the EU General Data Protection Regulation

Overview

The data subject access request, or DSAR, is the most widely exercised individual right afforded by the EU General Data Protection Regulation.[1] Predating the GDPR as a right codified in the Data Protection Directive of 1995,[2] the "right of access" (Article 15 of the GDPR) affords data subjects the presumptive right to request access to, or copies of, personal information about themselves held by a data controller.[3] In-scope information that is responsive to the request must be identified and delivered to a data subject in 30 days (or 90 days with potential extension), posing a significant challenge for organizations across the EU and UK.

Responding to DSARs from customers and clients can be complicated, and organizations should think about approaches and resources devoted to ensuring requests are adequately received, verified, and responded to. However, most organizations will have information management practices in place that, to some degree, allow for the relatively straightforward identification of the information the customer or client has requested.

In the case of employees or ex-employees, however, the scenario can be very different.

The amount of data falling within the scope of these requests can stretch far across the breadth of electronically stored information, from myriad file types and records to unstructured data sources, emails, and more. In many cases, this can encompass hundreds of GB of data and hundreds of thousands, or even millions, of individual emails and documents.

Scope of the Request

DSARs from current and former employees tend to be some of the most expensive from both a time and a resources perspective. Requests may require collecting data from numerous individuals within the company and may include internal company files and human resources documents. Employment disputes and other contentious issues arising in the workplace can often be a driver of employee/ex-employee DSAR requests, implicating performance reviews and documents related to workforce and resource decisions if containing specific information about the data subject.[4] Circumstantial or management-related information about whether the person is/was injured and on sick leave, and on what grounds, can be considered personal information, as can an individual's name, salary, and other details around compensation.[5]

DSAR-centric case law in the UK and elsewhere often provides a good indicator of what can happen when an employee response goes awry. In one notorious example, a response to a DSAR from an ex-employee, carried out amid ongoing employment litigation, dragged out over several years and implicated the review of 500,000 emails documents at a cost of £117,000 ($155,000). Despite the time and expense, the entire process resulted in the disclosure of only 33 responsive documents.[6]

It should be noted, too, that the requestor's motive in carrying out the DSAR is irrelevant to the requirement to respond to the request.[7] Accordingly, the fact that related employment litigation or an employment tribunal proceeding – which in the UK often involves disputes related to unfair dismissal, redundancy payments and employment discrimination – may be ongoing does not bar the requestor from seeking specific information in relation to the DSAR. However, certain information may be exempted from the response in some instances, as described below.

WHO IS THIS GUIDE FOR?

- CHRO/Human Resources Director
- Compliance Officers
- Data Protection Officer (DPO)
- Employment Law Attorneys
- GDPR Controllers and Processors
- In-house Counsel
- In-house Legal Staff
- Outside Counsel

Exemptions to the Response

Interestingly, the "right of access" is not an absolute right. There are exemptions to the response that an organization will want to ensure it has fully considered prior to disclosing any information to the data subject.[8] Exemptions are generally subject to individual member state law, and thus include variations in the types of information exempted from DSAR response from jurisdiction to jurisdiction. The UK's Data Protection Act (2018) also includes provisions exempting response in certain instances.

Examples of member state (i.e., Ireland) and UK DSAR exemptions most relevant in the employment context include:

The Irish Data Protection Act 2018 (Sections 60 – 61, 94):

- **Legal Claims** – where disclosure may interfere with the establishment, exercise, or defense of a legal claim, prospective legal claim, legal proceedings, or prospective legal proceedings.[9]

- **Civil Law Claims** – where disclosure may relate to any liability of a controller or processor in respect of damages, compensation, or other liabilities or debts related to the claim.[10]

- **Commercial Interests** – where information may involve estimating the amount of the liability of a controller in given claim, and would be likely to prejudice the commercial interests of the controller in relation to the claim.[11]

- **Confidential Communication** – the personal data relating to the data subject consists of an expression of opinion about the data subject by another person given in confidence or on the understanding that it would be treated as confidential.[12]

- **Legal Privilege** – the rights of data subjects may be restricted in order to avoid the obstruction or impairment of official or legal inquiries, investigations or procedures or the operation of legal privilege.[13]

Note that the above are Irish DSAR exemptions – other member states may have differing exemptions or no exemptions at all.

UK Data Protection Act 2018 (Schedule 2, Parts 3 and 4):

- **Information Relating to Other Individuals** – Data controllers in the UK are not obliged to disclose information to the data subject to the extent the disclosing information relates to another individual who can be identified from the information, UNLESS
  - The other individual has consented to the disclosure of the information to the data subject; or
  - It is reasonable to disclose the information to the data subject without the consent of the other individual.[14]

- **Legal Professional Privilege** – where a professional legal adviser to a client of the adviser owes a duty of confidentiality.[15]

- **Self Incrimination** – where compliance with the request would reveal evidence of the commission of an offence.[16]

- **Corporate Finance** – where personal data was processed for the purposes of or in connection with a corporate finance service (in the context of Condition A or Condition B):
  - *Condition A* – disclosure would be likely to affect the price of an 'instrument'.
  - *Condition B* – the relevant person reasonably believes disclosure of the personal data in question could affect the decision of a person

WHAT IS EMPLOYEE PERSONAL DATA?

'Personal data' means any information relating to an identified or identifiable natural person ('data subject'). Examples:

- Names
- Addresses
- IP Addresses
- Financial information
- Employee health data
- Login IDs
- Biometric identifiers
- Video footage
- Geographic location data

Learn more at ICO.org.uk

  - whether to deal in, subscribe for, or issue an instrument, or
  - whether to act in a way likely to have an effect on a business activity, with a potential prejudicial effect on the orderly functioning of financial markets or the efficient allocation of capital within the economy.[17]

- **Management Forecasts** – information processed for the purposes of management forecasting or management planning in relation to a business or other activity, and likely to prejudice the conduct of the business or activity concerned.[18]

- **Negotiations** – Exemption for 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.[19]

- **Confidential References** – Exemption for personal data consisting of a reference given (or to be given) in confidence for the purposes of the education, training, or employment of the data subject.[20]

As exemptions to DSAR disclosures can be complicated to apply and fraught with nuance, careful consideration of the data and documents at issue and analysis of any exemptions are critical to the DSAR process. An approach for identifying exemptions should be integrated into any workflow that focuses on DSARs from employees and ex-employees. It should also be noted that the burden is on the organization or data controller responding to the request to properly apply the exemption.

Employee DSARs a top data privacy complaint

In 2019, the first full year of implementation of the GDPR, data protection complaints related to DSARs were the single highest complaint category received by both the Irish and UK data protection authorities (29% and 38%, respectively). Further, in its 2019 annual report, the Irish data protection authority identified HR/employment disputes as a specific driver of complaints, with concerns about workplace surveillance and adequate response to employee DSARs among the topics, saying that, "Disputes between employees and employers or former employers remain a significant theme of the complaints lodged with the DPC, with the battle often staged around a disputed access request."[21]

Across the UK, businesses spend an average of £1.64 million ($2.1 million) on DSAR responses per year, with current and former employee DSARs taking up the most resources.[22]

AVERAGE SPEND IN THE UK

UK businesses spend an average of £1.64 million ($2.1 million) on DSAR responses per year, with current and former employee DSARs taking up the most resources.[1]

Applying a discovery approach to employee/ex-employee DSARs

As noted above, searching across the sheer volume of data in email, shared files, and even collaborative working applications can be a daunting task, and several DSARs in quick succession can overwhelm even the most diligent and prepared privacy and DSAR response teams.

However, the data collection, analytics, search optimization, and redaction tools so frequently handled by discovery teams can be hugely beneficial when applied to DSAR response. An experienced discovery team with a tried-and-tested solution for DSARs can help manage the process: from filtering data collections down to the sample most likely containing information on the data subject to assisting in identifying exemptions to tailoring disclosures to fit the request criteria of the data subject with exceptional precision.

A step-by-step approach utilizing discovery workflows is laid out below:

1. Narrow the initial collection to the scope of the request.

DSARs from employees and ex-employees, especially from legacy or upper-level management individuals, can result in data collections that quickly amass data from numerous sources and file shares across the company, resulting in extensive data volumes. Organizations should look to coordinate with data subjects to get a precise indication on the scope of the request, seek to eliminate any data that a requestor may already have access to, and eschew collections from backups or archives unless those are the only sources of data which may contain information responsive to the request. Narrowing data collections can streamline response times and reduce downstream costs. Organizations familiar with discovery should consider the nuance of DSAR requests and differentiate the collection process for DSARs from that of litigation, regulatory matters, or even legal holds. DSARs, in general, tend to be much more targeted.

2. Consider analytics and advanced document search approaches.

Data collections for DSAR response may be wide-reaching, but response windows are fixed and time is generally of the essence. Applying analytics and aggressive methods for de-duplicating documents is highly advisable. Using communication analysis or other techniques for honing in on documents potentially within scope of the DSAR can also offer huge advantages, with some efforts narrowing the largest document collections down by as much as 98%.

PENALTIES

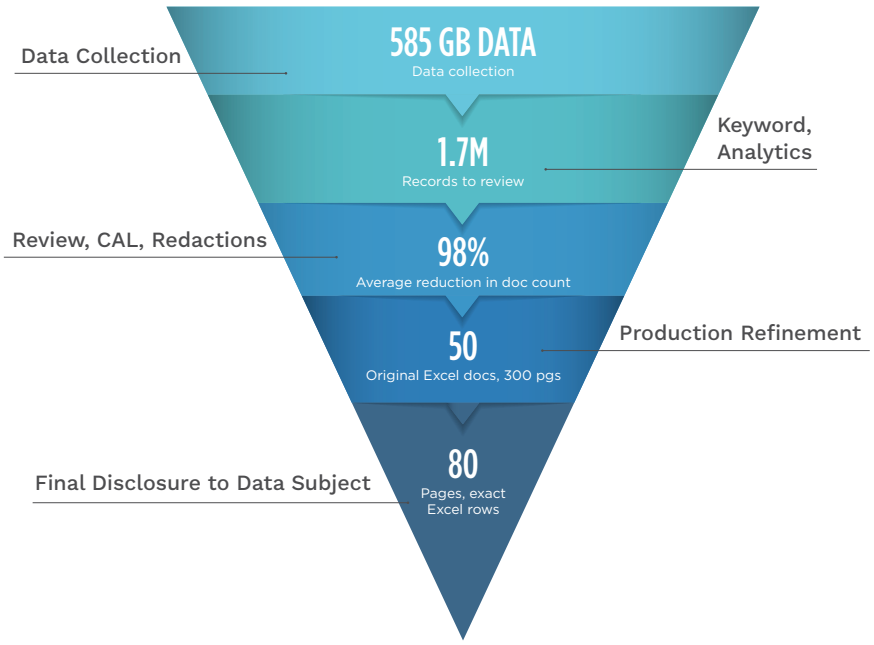
Failure to comply with a DSAR request from an employee or other requestor is subject to a fine from the ICO:

A maximum of €10 million or 2 per cent of the total annual revenue in the preceding financial year, whichever is greater.

3. Advocate for sophisticated document review techniques.

In most cases, a "search-hits-only" review will be preferable, concentrating the team's review of documentation only on search term and keyword hits themselves, ignoring any attachments or "document families" that do not contain those hits. Bringing in full families may be necessary for context, but generally won't be needed for the review itself.

Further, depending on the scope of the universe of documents for review and size of the review team in place, a continuous active learning review model may be preferable. CAL will not only afford the team an opportunity to begin reviewing immediately, but will also give early insights into the range of documents potentially containing the data subject's information and condense the amount of time necessary for review.



> "'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or by one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person".

4. Incorporate exemption identification and redaction into the review workflow.

Identification of the complicated and numerous exemptions indicated above can be woven into the review process, so that teams identifying documents containing information on the data subject can also indicate any potential exemptions that apply in a straightforward manner. Documents containing exemptions can be siphoned off and escalated to counsel or others to determine the applicability of exemptions and ensure these decisions can be supported later. Teams can also make a decision to redact any information that may be subject to an exemption but disclose the remainder of the document, if required. In fact, redaction can be a considerable element of the DSAR workflow, given that any disclosures to a data subject must remove references to other individuals or persons apart from the requestor.[23] As redactions on numerous documents can be a time-consuming process, approaches for streamlining the redaction process are advantageous, including inverse redactions (reverse redactions that can then be removed) and automated redactions via preselected lists of names or other criteria.

5. Tailor the production process to suit the request.

Unlike in discovery, where disclosing original records to opposing parties is required, in a DSAR, data subjects only have a right to obtain their own personal information. There is no obligation to provide complete original documents, and most teams will not wish to do so. Accordingly, implementing a process for providing document excerpts, extractions, and/or specific rows, columns or pages will be necessary and advantageous for the DSAR teams charged with the response. Fully redacted pages can be removed from individual documents, and line-by-line extractions of Excel files can be disclosed to the data subject. Utilizing a tailored production process will greatly refine the ultimate disclosure, eliminating nonresponsive pages or exempted bits of information from the output the data subject will receive.

Conclusion

DSAR requests from employees and ex-employees can be complicated and broad in scope. Organizations need to ensure that their process for these specific DSARs diverges from their DSAR response for customers and clients. Exemptions should be carefully considered and proper resources should be allocated to ensure an efficient and effective response, especially when contentious employment-related disputes may be an underlying factor in the request.

Discovery processes offer some well-established and tested solutions that can be effectively applied to the DSAR response context, and with a little creativity and collaboration, even the most contentious, sweeping, and complex requests can be sufficiently handled on a reasonable cost scale and well within the statutory timeline. DSAR requests that span hundreds of GB of data can seem daunting at first, but with adequate preparation and an approach through the discovery lens, a refined disclosure to a data subject within 30 days is very much within reach.

About The Author

RYAN COSTELLO, ESQ., CIPP/E/US

HEAD OF DATA PRIVACY ENGAGEMENT SERVICES

Ryan Costello, Esq., CIPP/E/US, is head of data privacy engagement services at ProSearch, a leading provider of comprehensive discovery solutions to corporate legal departments and law firms. A U.S.-licensed attorney and expatriate based in Europe for more than 10 years, Costello has cultivated expertise in data protection and data privacy compliance. He assists organizations in remediating cross-border discovery risks, utilizing data management solutions, and innovative technologies.

External Sources Cited

[1] See Irish Data Protection Commission (DPC) Annual Report, Jan. 2020, pg. 19

[2] Article 12 of the DPD; https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:html

[3] Regulation (EU) 2016/679, General Data Protection Regulation (GDPR), Article 15

[4] See Irish DPC Annual Report, pg. 7; see also *Nowak v Data Protection Commissioner*, CJEU (December 2017), comments made about a data subject related to an examination or review constitute personal data.

[5] See relevant EU case law: C-*101/01 Criminal Proceedings against Lindqvist* (Sweden, 2003) and *C465/00 Rechnungshof v. sterreichischer Rundfunk* (Austria, 2003).

[6] See *Deer-v-University of Oxford [2017] EWCA (Civ) 121.*

[7] See *Ittihadieh v Cheyne* [2017] EWCA Civ 121 (heard together with *Deer* on Appeal from the High Court, Queen's Bench Division].

[8] GDPR Article 23

[9] Irish Data Protection Act 2018 – Part 3, Chapter 3, Section 60(3)(a)(iv)

[10] *Id* at Section 60(3)(a)(v)

[11] *Id* at Section 60(3)(a)(vi)

[12] Id at Section 60(3)(b)

[13] *Id* at Part 5, Section 94 (3)(i)

[14] UK Data Protection Act, Schedule 2, Part 3, Section 16(1) – (3)

[15] *Id* at Part 4, Section 19

[16] *Id* at Part 4, Section 20

[17] *Id* at Part 4, Section 23

[18] *Id* at Part 4, Section 24

[19] Irish DPC Annual Report, pg. 19

[20] https://guardum.com/wp-content/uploads/2020/05/PowerPoint-Guardum-DPOs-Guardum-branded-2-1.pdf

[21] *Id* at Part 4, Section 21 (1) – (5)

[22] *Id* at Part 4, Section 22

[23] GDPR Article 15 (4)

PROSEARCH
LOVE WHAT YOU DISCOVER

ProSearch is a leading provider of comprehensive discovery solutions to corporate legal departments and law firms, empowering them to better manage their portfolio of matters for improved legal and business outcomes. With advanced technologies, innovative workflows, and deep expertise in deriving insights from data, ProSearch enables teams to better respond to litigation, investigations, and regulatory and compliance actions. ProSearch reimagines the conventional approach to solution design and service delivery, helping clients to take control of their discovery processes by staying focused on legal and strategic issues while reducing the risk and costs associated with discovery.

www.ProSearch.com | 877.447.7291 | info@ProSearch.com