



# SARIMA

## INTRODUCTION TO DATA SUBJECT ACCESS REQUESTS



## Executive Summary

The introduction of new regulations creates obstacles for lawmakers worldwide and the EU General Data Protection Regulation (GDPR) was no exception. There is a huge volume of information publicly available on the GDPR in general, and also specifically in relation to the right of access by the data subject under Article 15, otherwise commonly known as Data Subject Access Requests or DSARs. While this paper will not provide an in-depth education on GDPR or DSARs specifically, it will introduce ways to optimise workflows to address DSAR challenges.

## Regulatory Background

The GDPR has applied from the 25th of May 2018 and is directly applicable to EU member states without local laws in place, but it does have room for derogations. The UK Data Protection Act 2018, for example, sits alongside the GDPR and tailors how it applies in the United Kingdom.

It is worth noting that the GDPR is principle based, so there is some flexibility of interpretation that can result in different points of view being quite reasonably espoused or adopted, subject to any official guidance or case law already in place under the existing law. In relation to the case law around DSARs, it is still common to refer to precedents decided under the previous regime that include findings such as:

- That searches are obligatory, but organisations can apply proportionality to them appropriately
- That secondary purposes, such as concurrent employment proceedings that are in progress— are generally irrelevant in terms of refusing to respond to a DSAR;
- The fact that any privilege review should be a targeted one, and not construed more broadly; and finally
- Guidance on how to approach data that contains the personal data of both the requesting data subject and that of other individuals, otherwise known as mixed personal data



Several other articles and recitals complete the picture, Article 12 and Recitals 59, 63, and 64 in particular. Article 12 sets out, inter alia:

- Personal data to be provided in writing or by other means, including electronically
- A one-month time limit to respond in most cases, extendable by up to two further months where complex and/or multitudinous
- A requirement to identify the data subject, as releasing personal data to the wrong individual could be a data breach

Focussing in more detail now on DSARs, the requirements are set out in some detail in the GDPR. In the first instance, there is a focus on the data, dealing with those DSARs that are demanding in respect of personal data contained in unstructured documents. The second main requirement is the need to supply transparency information alongside this data, including, for example, the purposes of the processing, the categories of personal data concerned, and more.


It is worth noting that there is significant overlap between this transparency information and the notice information that organisations should already have supplied under Articles 13 or 14 (as appropriate), as well as overlap between the information required in all of these articles and Article 30, the written records of processing activity that organisations should already have in place.



## New Challenges

It is a fair observation that many of the requirements around DSARs have not changed immensely, but it is worth noting that the GDPR has introduced some new challenges, including:

- The elimination of the cost barrier for a data subject to submit a DSAR in most circumstances;
- The need for a request to be in writing has been removed, making oral requests, for example, now acceptable;
- A reduction in the timeline to respond from 40 days to one month, compressing response timelines unless an extension can be justified;
- An express requirement that the rights and freedoms of others are to be considered during the process, which can be of particular concern when dealing with mixed data;
- An increase in the list of transparency information data subjects are entitled to; and
  - Elimination of Cost Barrier and Requirement to be in Writing
  - Reduction of Timelines from 40 days to 1 month
  - Rights and Freedoms of others to be Considered
  - Increased list of Transparency Information
  - Increased Awareness of Data Subjects around their Rights



A climate of increased awareness around data subject rights in a social media driven world, which potentially increases the burden on organisations in terms of administration costs, reputational risk, and potential public scrutiny.

There are also anecdotes of multiple DSARs arriving on the same day, to the same organisation, all on the same standard template, which may indicate weaponisation. This has in turn created an additional challenge for many organisations looking to meet their duties and obligations, particularly around responding to DSARs in an efficient and cost-effective manner.



## Preparatory work

Those who have read the details of the GDPR may have noticed a pervasive theme running through the text encouraging the effective use of technical and organisational measures. The intention here is for organisations to harness not only technology, but also people and processes to address the challenges posed in continuing steps towards compliance.

Breaking these steps down into proactive and reactive activities can be helpful. It is fair to infer that the better prepared an organisation is, the easier it will be to react.

This preparatory work is potentially more pivotal when dealing with organisations where DSARs have the potential to be:

- Complex, involving unstructured data from multiple sources and of various formats; or
- Voluminous, needing an efficient, repeatable and defensible process.

Customer data may be structured or unstructured. If it is structured, it may have fields containing longer elements of binary or character information that would otherwise be considered unstructured data; for example, this could include call centre recordings. Similarly, some employee data may be in structured systems.



Ensuring that the organisational data estate is under management including:

- Data discovery
- Data mapping (primarily Article 30 Records of Processing Activities in a GDPR context)
- Providing Privacy Notices
- Carrying out Data Protection Impact Assessments

Responding appropriately to point of impact events including:

- DSAR requests
- Other exercises of data subject rights (such as the Article 17 right to erasure)
- The potential need to act on a data breach in 72 hours
- Ceasing processing where appropriate where Consent is Withdrawn





## Types of DSAR

### Employment DSARs

- Potential to be both complex and voluminous
- Have a particular focus around unstructured data
- Very real chance that they may be part of, or develop into, an Employment Tribunal case

### Customer DSARs

- Potentially greater in number, but generally a little less complex
- Much of organisations' customer data is more likely to be in structured systems
- This includes relational databases, in respect of which it is often possible to pull more targeted reports or exports down from.



Unstructured data potentially falls into the category of “dark data,” a term frequently applied to electronic information within an organisation that is not easily searchable or accessible. This data is likely to not only be in an unstructured format, but also to be unclassified, and potentially unmanaged by current information governance solutions.<sup>2</sup>

Information governance of this type of data in organisations' document storage and management environments will often involve high-level categorisation. This might involve the use of regular expressions and other similar techniques to identify areas in the data estate that potentially contain personal data, an exercise perhaps carried out as a result of previous efforts to prepare for the GDPR and populate Article 30 records of processing.

For certain types of data, such as emails, it may also be possible to resolve entities to the level of an individual person or data subject, which will consequently help target and streamline DSAR efforts when a specific request is received.

<sup>1</sup> Holyoake v Candy [2017] EWHC 3397 (Ch), Dawson-Damer v Taylor Wessing LLP [2017] EWCA Civ 74, Ittihadieh v Cheyne Gardens RTM Company Ltd and others [2017] EWCA Civ 121, Deer v University of Oxford [2017] EWCA (Civ) 121, DB v The General Medical Council [2018] EWCA Civ 1497,



## Leveraging SARIMA to optimise workflows for DSARS

Organisations that have prepared will almost certainly be in a better place to respond. Sarima.io is an on-premise application that enables organisations to scan large quantities of unstructured data for a particular identifier(s). Sarima performs with minimal system resources and can scale effectively thanks to the unique logic that Sarima leverages to scan data (Python) . Sarima scans large data sets efficiently, and faster than any other technology available on the market with a 0% 'false-positive' rate. Sarima also provides the file name (and location of a file) that contains a particular identifier and presents it in a report for redaction or any other operational task, such as file open, copy, delete and archive. We support all Microsoft formats including but not limited to .docx .pdf .xls .txt more.

## Conclusion

Whatever organisations adopt as their point of view around DSARs and their approach to data protection and privacy, they should consider refining their approach as they go. With an eye on the regulators and courts, and, given the continuing accountability requirements, organisations should be sure to record what they did and why they did it, as it may help if someone down the line doesn't agree with their approach and they find themselves in a discussion with the regulator or in some other public forum, e.g. court or social media. With Sarima, organisations are able to quickly discover unstructured data, easily reveal the relevant underlying information, and collaboratively act on requests in a timely manner.

Looking for more information?

Contact us at [sales@sarima.io](mailto:sales@sarima.io)

Website: [www.sarima.io](http://www.sarima.io)

