Right of access- Report

January 2020

1 Report summary

1.1 Introduction

The General Data Protection Regulation came into force May 25th, 2018 and arguably one of the most challenging elements of this regulation is that of a data subject's "right of access".

The "right of access", commonly referred to as "subject access", gives individuals the right to obtain a copy of their personal data from you, a Subject Access Request (SAR), as well as other supplementary information. It is a fundamental right for individuals. It helps them understand how and why you are using their data and enables them to check that you are doing it lawfully.

1.1 SARs – the facts!

- ✓ **Under GDPR, any individual can write to you and ask for a copy of all the personal information that you have about them**
- ✓ **Organisations are obligated to service SARs promptly:**
  - **you must be able to service the request within one month of receipt; and**
  - **return all of the information in an easily accessible format.**

To date, the Information Commissioner's Office (ICO) does not appear to have sought to enforce this aspect of the regulation too strongly. However, with the latest draft guidance on the "right of access" being published for consultation, it is perhaps an indication that as we commence this new decade it is a topic that will begin to attract a higher degree of scrutiny, not only by them but the public at large.

Infoboss has conducted cross-sector research to help inform the debate. Drawing on our research findings and our review of the ICO's draft guidance, this report provides context to the problems of servicing the "right of access" along with practical advice to help an organisation to better prepare to meet its regulatory responsibilities in servicing a data subject's "right of access".

1.2 About our research

We adopted both quantitative and qualitative research in the form of surveys and one-to-one interviews with organisations of varying sizes and complexity on their understanding and approach to "right of access". We also collated commentary from the related research findings of other organisations. Finally, we incorporated personal and third-party experiences of submitting SARs and receiving responses, a mystery shopper role, to provide context as to what is actually happening on the ground.

Our objective in undertaking this research was to understand the reality of current processes for servicing SARs and the effectiveness of these processes in practice. In so doing, provide insight into the challenges ahead and how best an organisation may prepare to tackle them.

1.3 Conclusions from the research

From the report's findings, we summarily concluded the following…

- Organisations that are classified as business to consumer (B2C) are better prepared to service SARs than Business-to-business (B2B)
  - From our research it is worth noting that B2B organisations generally do not get SARs and this may account for their lower level of preparedness.
  - B2C organisations though prepared, were not as efficient as they perhaps could be.
  - It is worth noting that when the ICO publish their new guidance paper on the "right of access" later in 2020 there is likely to be an increasing focus and potential burden

on organisations to service a greater number of SARs and perhaps to a greater depth of response than has taken place to date.

- 71% of organisations that get SARs have seen an increase in demand since the GDPR deadline May 2018
    - Separate research by Parseq puts this figure at 62%
- Organisations that get SARs spend on average 709.5 days per year servicing them!
    - The average number of SARs received per annum (by those that get them) is 55
    - The average time to service a SAR is 12.9 days
    - Other research puts the processing figure at a much lower level, but we believe this is skewed by including greater numbers of B2B companies in the results.
- Parseq's research suggested that 87% of organisations have challenges servicing a SAR. From our research, the most challenging aspects of servicing a SAR in priority order are:
    - Finding and collating information;
    - Redaction; and
    - Administration
- This was perhaps explained by the finding that over 2/3 of the data analysed to service a SAR was sourced from unstructured data sources like email, shared drives and document management systems. That said, from those receiving SAR information from organisations, very few were actually getting anything returned other than data from structured data sources.
- The methods being adopted for finding and collating data to service a SAR such as scan based searching (often with different tools requiring specific skills to use them) are perhaps a significant contributor to the time taken to service a SAR.

The complexity of an organisation's data estate and in particular the number and scale of unstructured data sources used to hold customer data are significant contributory factors to the time required to service SARs. Organisations are generally not providing a full and complete set of data when requested (primarily because they are unable to do so across the harder to reach unstructured data sources). Complex SARs, legal and/or employee related ones that involve the need to interrogate emails and meeting minutes etc. often take significantly longer to service (anecdotally times in excess of 90 days are not uncommon)!

Current organisational SAR processes are unlikely to be able to cope with an increase in SARs, especially if the need to source unstructured data in responses to a request is enforced. Our research suggests that the most likely approach that an organisation would take in this eventuality would be to recruit more staff. From our findings, we do not believe that this will solve the problem and could in fact make it worse and run the risk of an organisational data breach from utilisation of inexperienced staff in the finding, collation and redaction processes with resulting fines and reputational impact.

Alternatively, putting in place a system (such as Infoboss) that can collect, classify and store data from across the entire data estate and in turn enable a simple search and collation mechanism for data required to service a SAR, can significantly reduce the servicing time for a SAR. Potentially reducing the cost of servicing SARs in the short term and underpinning a SAR process that is simple, efficient, provides an enhanced customer experience and can scale without a significant increase in costs or human resources to service higher volumes of SARs if the organisation is required to do so.

2 ICO guidance on the “right of access”

The recently published draft guidance on the “right of access” is a comprehensive document providing answers to questions that naturally arise when an organisation is seeking to establish efficient and effective SAR servicing processes. The paper provides, several working examples to bring business context to the guidance and a short summary of the objectives of this paper are outlined here…

Whether or not you receive SARs on a regular basis, it is important that you are prepared for and able to take a proactive approach to servicing them. This will help you to respond to requests effectively, efficiently and in a timely manner.

The ICO guidance will help your organisation to:

- comply with your legal obligations under the GDPR and Data Protection Act 2018 (DPA 2018) – and show how you have done so;
- streamline your processes for dealing with SARs, saving you time and effort;
- increase levels of trust and confidence in your organisation by being open with individuals about the personal data you hold about them;
- enable customers, employees and others to verify that the information you hold about them is accurate, and to empower them to inform you if it is not;
- improve confidence in your information-handling practices; and
- increase the transparency of what you do with individuals’ data.

Fundamentally the ICO would like you to prepare your organisation to handle SARs efficiently and effectively. It is very much in your interests to do so! Not just from a regulatory compliance perspective but also to ensure the process does not adversely impact your business operations, customer service and financial performance. Summarily, it is an opportunity to provide a unique and positive experience for your customers, showcasing your fantastic customer service.

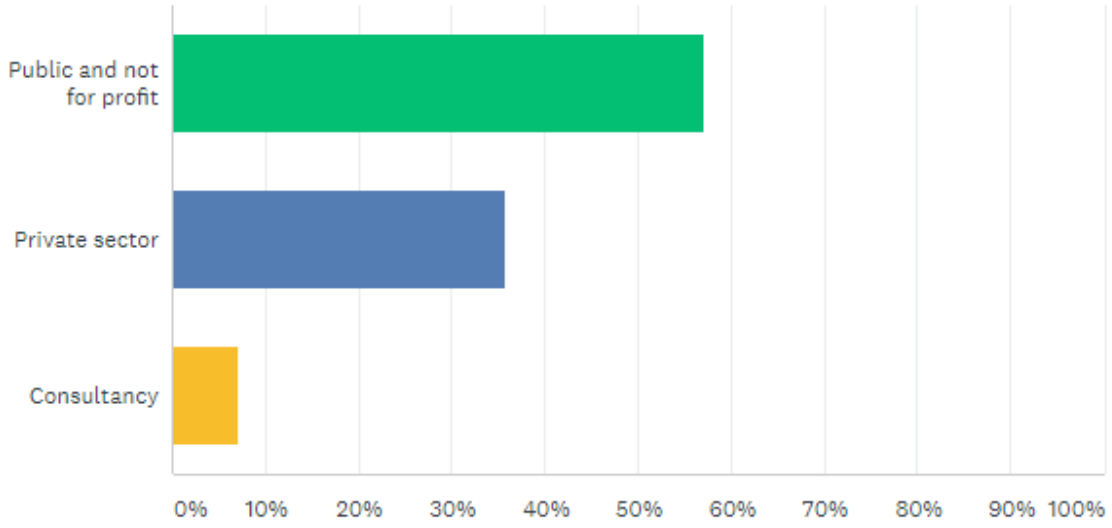
You can access the ICO guidance and consultation on “right of access” via the following link:

https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/ico-consultation-on-the-draft-right-of-access-guidance/

3 Infoboss research

3.1 Participant demographics

Our research has included organisations from across the public and private sectors as well as consultancies and other professional service bodies that deliver services to both.



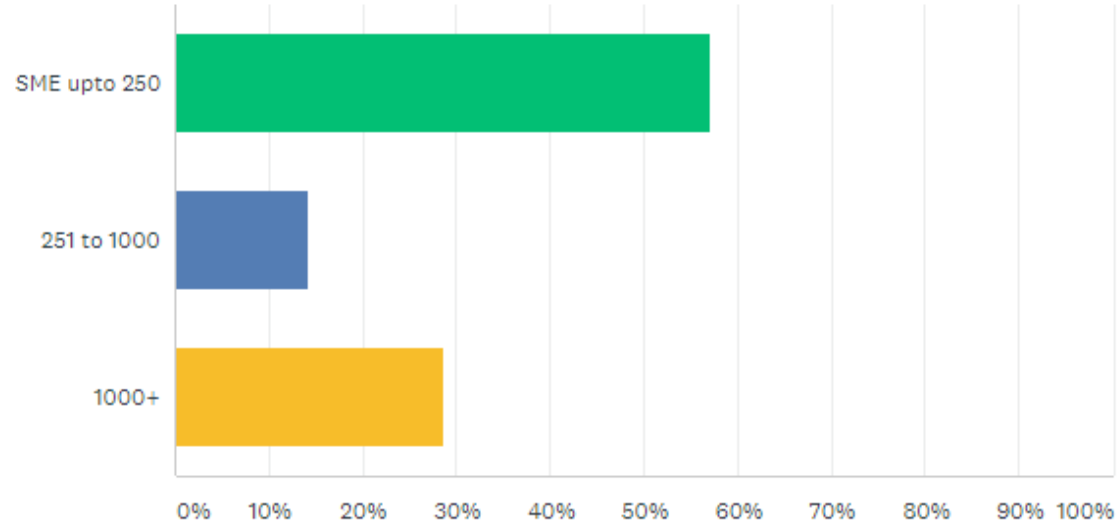
3.2 Type of organisation by target customers

Almost 60% of the organisations we researched were business to consumer (B2C). There is a very different level of preparedness apparent between B2C and B2B companies. B2C businesses are more likely to receive SARs from members of the public. Whereas B2B businesses are realistically only likely to receive SARs from current or former employees. The scale of the demand and requirement is very different and is reflected in the SAR processes that each type of organisation has put in place.

However, we believe there is an inherent risk in assuming that if you're a B2B organisation that you won't get SARs. It is feasible and dare we suggest likely that you will get SARs from employees or former employees (especially for large employers with high staff turnover) and given the nature of the challenges in servicing them such requests could potentially result in significant effort to resolve if the systems and procedures to do so are not in place.

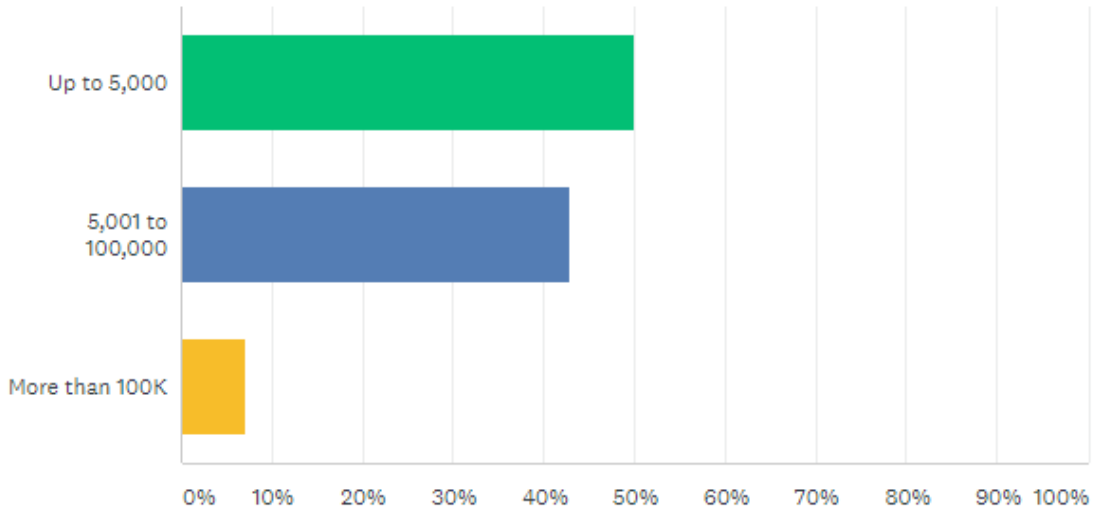
3.3 Number of employees

Just over half of our research was conducted with organisations employing fewer than 250 staff. This threshold of employee numbers is typically one that is associated with Small Medium Enterprises (SMEs). Our research has revealed that SMEs have exactly the same challenges in servicing SARs as larger organisations. Interestingly however, the time to service a SAR is typically shorter in duration for SMEs than larger organisations. This is perhaps symptomatic of the complexity and scale of the data estate and the fact that its typically a senior experienced resource involved in servicing the SAR at an SME – i.e. someone who knows where to look and what and how to redact the resulting material.

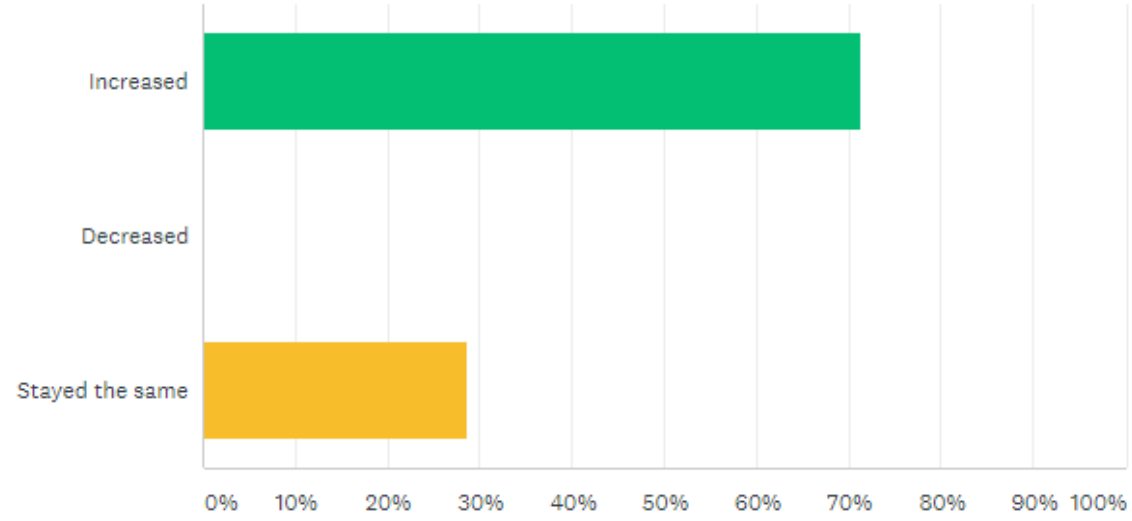


3.4 How many customers does your organisation have?

Approximately 50% of the organisations participating in our research had up to 5,000 customers, with 42% having 5,000 to 100,000. Around 8% had in excess of 100,000 customers each.



3.5 Since GDPR 25th May 2018 the number of SARs has…?



We can clearly see that our research supports the view that there has been an increase in SARs since the GDPR deadline of May 2018. Indeed 71% of business from our research have seen an increase in SARs over this period! This is a view that is further endorsed by research from Parseq which shows 62% of businesses in London have seen an increase in SARs over the past year.

It is however worth mentioning that from our research B2B organisations and B2C organisations that generally don't get a lot of (if any) SARs have seen little or no change in demand. When interviewed and pressed we discovered that these organisations have an assumption that they wouldn't get many (if any) SARs and therefore have not invested in putting robust processes to service them in place.

As a cautionary tale, we were made aware of at least one organisation that was receiving two SARs per month each taking no longer than 2 weeks to service. They had one member of staff trained in servicing SARs in what appeared to be a very inefficient process. A short time later, a "no win, no fee" solicitor was chasing their customers for a class action which resulted in a five-fold increase in SARs. The organisation had to take on a further four members of staff in a short timescale to service the resulting demand!

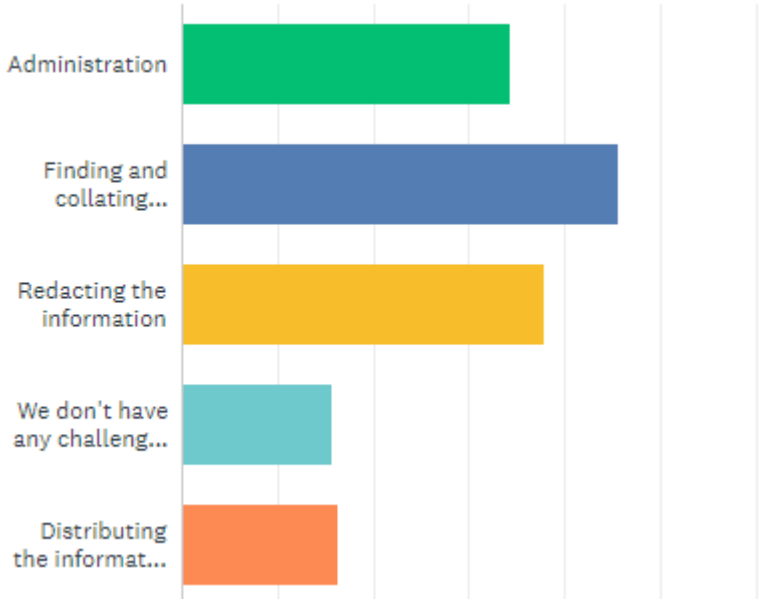
3.6 How many SARs?

We asked the question as to the number of SARs per year the organisation receives. The average number (of those getting them) was 55, with the lowest being 10.

The B2B organisations we engaged with had not received any SAR requests in the period. However, we believe that it is dangerous to assume that this will always be the case. Our research has indicated a distinct level of unpreparedness by B2B organisations for SARs and should they begin to receive them, we believe they would be unlikely to service them effectively or efficiently.

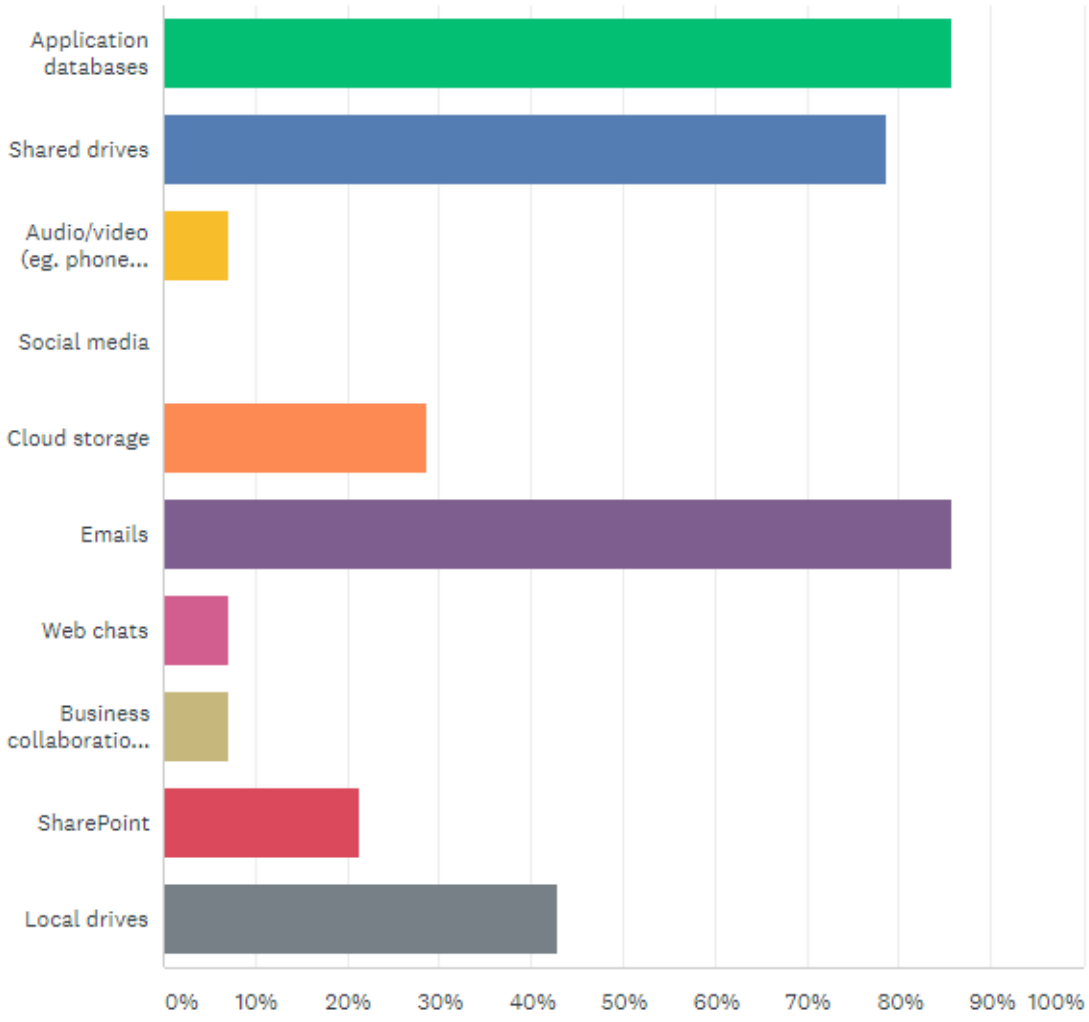
3.7 The most challenging aspects of servicing SARs?

We asked organisations to rank aspects of servicing SARs that they perceived to be the most challenging for them. The most challenging aspect was the organisation's ability to find and collate the information to service a SAR, followed by the redaction process and administration of the SAR process itself, in that order.



Parseq's research discovered that 87% of London businesses had suggested that servicing a SAR was a challenge. We asked this question to try to understand the problems that organisations were having when servicing SARs. Clearly the biggest appears to be that of finding and collating data to service a SAR. This in our view is by far and away the most significant issue especially when looked at in the context of the answer to the question posed as to where data is within the organisation that is used to service a SAR…

Finding information in unstructured data sources is often a labour-intensive exercise. Furthermore, in extreme cases it literally involves a person opening and reading documents, emails or viewing files to determine if they are related to the data subject making the request. More often people are using scan-based searches within email or file systems to endeavour to find information. But these methods can compound the problem especially when we look at the variety of system types where data is to be sourced from to service a SAR…



Each one typically requires a different tool or variant of the same tool to service a SAR. This greatly increases the skills needed and costs of the resources to service the SAR.

Finding and collating information for a SAR is a problem that Infoboss solves by indexing all data from data sources into a single searchable repository enabling fast Google™ style searching across all relevant data sources to identify and collate information on the data subject into a ZIP file ready for the person responsible for redaction to process.

The second biggest challenge cited was that, having found the data, then having to review and redact it before it can be returned to the data subject. On further questioning many reported this was an accepted issue because it was necessarily a skilled resource that was required to review the data before it was released.

The third most significant challenge was that of administration of the SAR process itself. Many had adopted a simple spreadsheet-based administration process which have sufficed to date, but all recognised the potential need for a system designed specifically for the purpose of administering such requests in the future.

3.8 How many days to service a SAR?

Putting it all together the average time to service a SAR from our research is 12.9 days. Given our earlier discussion about the challenges experienced in servicing SARs this would indicate a very real risk to the organisation if there was a significant increase in SARs. Based on our average number of SARs (55) and average time to service (12.9 days) then the average time spent servicing SARs in a B2C organisation is circa 709.5 days per annum!

One respondent commented that the "maximum time legally allowed" was taken in all cases. We know this is supposed to be one-month, but the respondent admitted that they had not been averse to seeking extensions in the past. They are not alone, many participants interviewed admitted to complex legal [SAR] cases involving significant resource and time to service. It is not uncommon in some sectors for this to be up to 90 days or more! This is potentially a risk for B2B organisations that do not have efficient processes for servicing employee SARs. These are likely to be litigious in nature and as such could be a significant challenge to service if the organisation was to suddenly start receiving a number of them.

It is perhaps fair to say that if your organisation is B2B you are more likely to receive a SAR from an employee or former employee than a member of the public. This is especially true if there is a high staff turnover at the organisation or there are disgruntled employees. However, if your business processes [B2C] data on behalf of a Data Controller (B2C organisation), then you need to be prepared to be able to service a request on behalf of the controller and probably in a much tighter timescale than that afforded to the controller themselves.

Anecdotally, some organisations had been starting the time to service a SAR from when they had confirmation from the data subject that the person making the request is in fact them. We understand that the ICO are seeking to tighten this process up and the time to secure confirmation will be included in the total time allowed.

3.9 What steps should you take?

There are several ways that you can better prepare your organisation for SARs. What is appropriate for your organisation depends on several factors, including:

1. The type of personal data you are processing;
2. Where it is stored;
3. The number of SARs you receive; and
4. The size and resources of your organisation.

Our report recommends ways that you may better prepare to service SARs.

The following list is not exhaustive:

- Awareness – Make information available about how individuals can make a SAR (e.g. on your website, in leaflets, in your privacy notice). Make it clear what the process is and what you expect them to supply to be able to service their request effectively.
- Training – Provide general training to all staff to recognise a SAR and what to do if they receive one. Remember, you only have one month from the date it was submitted to service it.
    - Provide more detailed training on handling SARs to relevant staff, dependent on job role.
- Guidance – Create a dedicated data protection page for staff on your intranet with links to SAR policies and procedures.

- Request handling staff – Appoint a specific person or central team that is responsible for responding to requests. Ensure that more than one member of staff knows how to process a SAR so there is resilience against absence.
- Asset registers – Maintain information asset registers which state where and how personal data is stored. This helps speed up the process of locating the information required to respond to SARs.
    - Or implement a system such as Infoboss to collect and classify the information required to service a SAR into one searchable repository.
- Checklists – Produce a standard checklist that staff can use to ensure a consistent approach is taken to SARs.
- Logs - Maintain a log of SARs you have received and update it to monitor progress. The log may include copies of information supplied in response to a SAR, together with copies of any material withheld and why.
- Retention and deletion policies – Have documented retention and deletion policies for the personal data you process. This helps to ensure that you don't keep information longer than you need to and therefore potentially reduces the amount of information you need to review when responding to a SAR.
    - Infoboss can be used to monitor your data estate to ensure a consistent approach is applied to data retention for all categories of data.
- Security – Have measures in place to securely send information. For example, by using a trusted courier or having a system to check email addresses before sending.

3.10 What about your information management systems?

You will find it difficult to deal with SARs effectively without adequate information management systems and procedures. Given that subject access has been a feature of data protection law since the 1980s, your information management systems should facilitate dealing with SARs by enabling you to easily locate and extract personal data. Your systems should ideally also be designed to allow you to redact third party data where necessary.

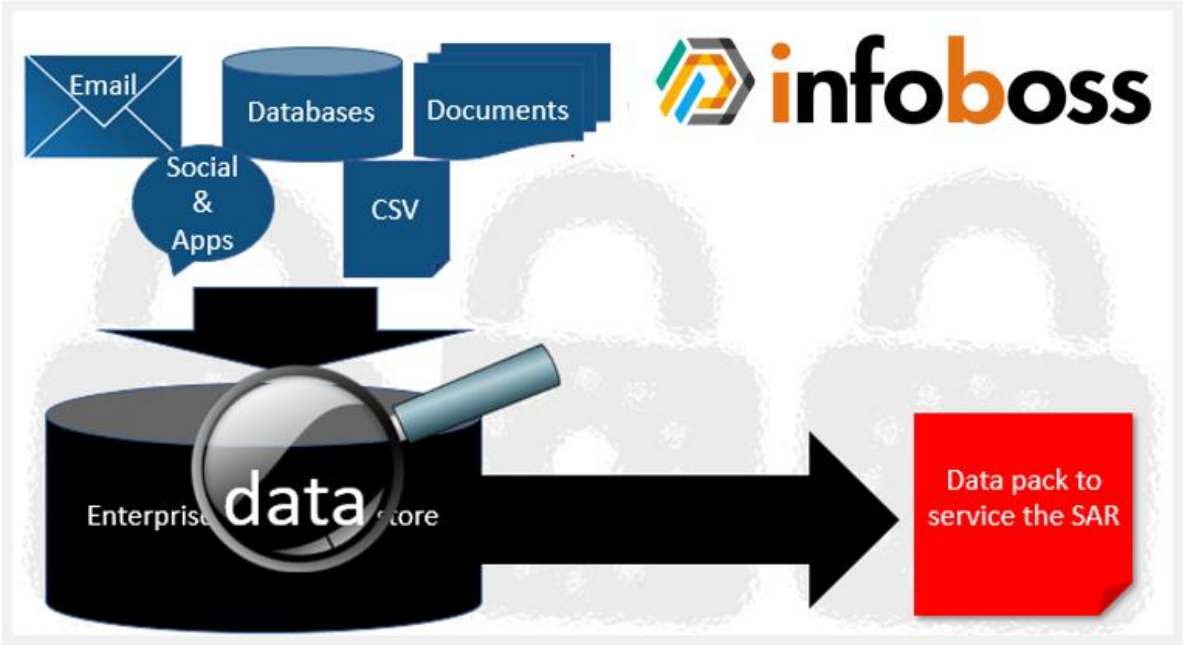
If you are implementing a new information management system, you need to take a 'data protection by design and default' approach and ensure that the system facilitates dealing with SARs. You should also have effective records management policies. For example:

- a well-structured file plan;
- standard file-naming conventions for electronic documents; and
- a clear retention policy about when to keep and delete documents.

This will assist you with your accountability and documentation obligations.

4 About Infoboss – our subject access solution

Infoboss collects data from any enterprise data source. We use a variety of techniques to analyse the data: Meta data or full file content scans (including OCR analysis of images that contain text), database record sets, emails (and attachments) and more. We store the data in an indexed and searchable format empowering your SAR servicing personnel with the tools necessary to quickly and efficiently locate the information for a SAR and export it to a ZIP file for further processing such as redaction or distribution to the client.



You simply let us know what data sources you'd like us to include and we'll configure and setup the system ready to process your SARs. All we require from you is remote access to a machine within your network to install the software onto with appropriate permission to enable access to the data sources in scope.

The software is designed with the specific purpose of empowering your SAR servicing personnel with the tools needed to quickly search and locate the information held on a data subject across all your enterprise digital data sources. Once data has been collated it can be easily exported (to a zip file) for subsequent redaction and further processing before returning to the client.

In a nutshell, we enable you to:

- Search and locate information from anywhere across your enterprise digital data estate;
- Easily identify and collect requested data about the individual; and
- Export the data and any attachments for subsequent redaction and distribution