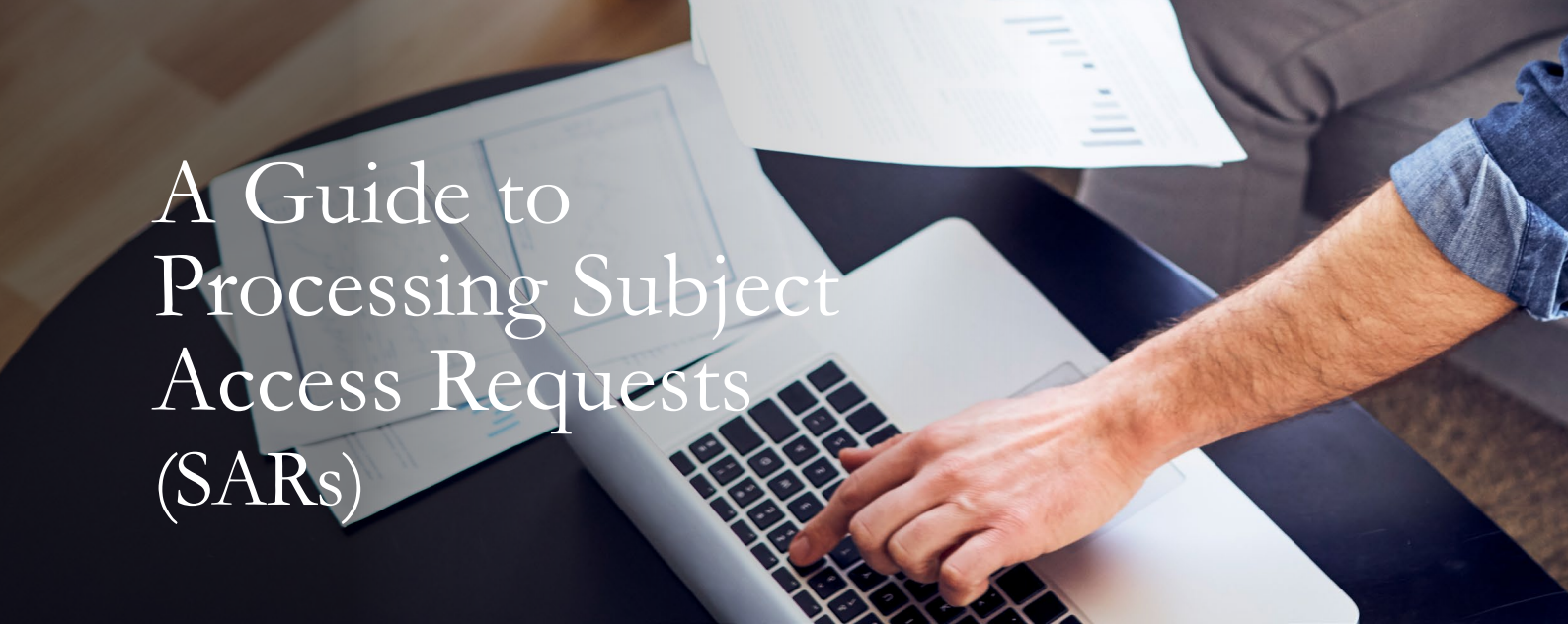

# A Guide to Processing Subject Access Requests (SARs)

Since the introduction of the GDPR in May last year individuals have become much more aware of their rights of access to their personal data. It is therefore extremely important that you have a clear action plan in place to process SARs within the short statutory timescale and so avoid fines or censure. In this article we address the SAR requirement, the practical impact of them and provide some top tips for dealing with these.

## The requirements

Article 15 of the GDPR sets out the legislative "Right of Access by the Data Subject" as follows:

"The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

**a.** The purpose of the processing

**b.** The categories of personal data concerned

**c.** The recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations

**d.** The envisaged period for which the personal data will be stored, or if not possible the criteria used to determine that period

**e.** The existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of the personal data concerning the data subject or to object to such processing

**f.** The right to lodge a complaint with a supervisory authority

**g.** Where the personal data are not collected from the data subject, any available information as to their source;

**h.** The existence of automated decision-making, including profiling"

Art 15.3 -The Controller shall provide a copy of the personal data undergoing processing.

Click here for ICO guidance on Subject Access Requests.

## Can you extend the statutory time period for response?

Only if the request appears complex, or the data subject has made several requests. If so, you can extend the time for response to two months but you must notify the data subject if you intend to do this and be able to justify doing so (you may have to explain this if the data subject complains to the ICO). As a rule you will need to reply to the vast majority of requests within one month.

## What are data subjects entitled to?

Data subjects are entitled to obtain the following from you:

- Confirmation that you are processing their personal data;
- A copy of their personal data; and
- Other supplementary information listed in Article 15 (largely covered by your privacy notice).

Personal data (as defined in the GDPR) will typically include name, address, telephone number, email address, and any other data which will be determined by the type of services you provide (e.g. national insurance numbers etc). You may also be processing special category data like criminal records and convictions data.

The ICO published guidance (click here) helps businesses determine what personal data they hold.

## Do you have to send a full copy of everything on the file?

No, providing a copy of the personal data does not mean that you have to copy the entire file – just the actual personal data.

## Remind Employees To Take Care

It is really important to remind your employees that anything they record in writing, including in email or file may potentially be disclosable under a SAR. The general rule should be that you should not write down anything you would not want an individual to see.

## What if the data includes information on other individuals?

The DPA 2018 says that you do not have to comply with the request if it would mean disclosing information about another individual who can be identified from that information, except if:

- The other individual has consented to the disclosure; or
- It is reasonable to comply with the request without that individual's consent.

In determining whether it is reasonable to disclose the information and what should be withheld (e.g. redacted), you must take into account all of the relevant circumstances, including:

- Any duty of confidentiality you owe to the other individual;
- Any steps you have taken to seek consent from the other individual;
- Whether the other individual is capable of giving consent; and
- Any express refusal of consent by the other individual.

If the other individual consents to the information being released then it would be unreasonable not to do so.

## Can you refuse a request?

Yes, but only in very limited circumstances you must be able to show justification for doing so. You can refuse to comply with a request if it is 'manifestly unfounded or excessive', taking into account whether the request is repetitive in nature. In such cases you can request a "reasonable fee", to be paid before dealing with the request (based on the cost of processing the request); or refuse to deal with the request. If you intend to charge a fee you should notify the individual promptly.

## Exemptions

The DPA 2018 contains a number of exemptions to the obligation to disclose, arguably the most relevant is where a duty of confidentiality is owed to clients.

Other notable exemptions include references given in confidence, personal data processed for the purposes of management forecasting or planning and negotiations between employer and employee.

Click here for further information on exemptions.

## What should you do when you refuse to comply with a request?

Inform the individual without undue delay and within one month of receipt of the request. Confirm your position and advise them of:

- The reasons why you are not taking action;
- Their right to make a complaint to the ICO or any other supervisory authority; and
- Their ability to seek to enforce this right through a judicial remedy.

You should also provide this information if you request a reasonable fee or need additional information to identify the individual.

## What if the client is deceased?

Data relating to deceased individuals is not personal data and is not subject to the requirements of the GDPR. You may, however, receive requests for information from others (such as relatives or executors of an estate). You will need to verify the identity of the individual requesting the data and the basis of the request before releasing information.

## What form of response?

If requested electronically then you can respond electronically unless a specific format has been requested by the data subject. Be mindful of security – send information encrypted/ password protected wherever possible – anything being sent by post should be sent by traceable delivery method.

## The response

Your final response in whichever format must contain the following:

- All of the information set out in Article 15.1. Much of this information will be contained in your privacy notice. You can refer to your privacy notice in the letter or attach a copy.
- Details of the source of the data if you didn't collect it directly from the data subject.
- Details of any information you have not included and the reason why.
- A statement that the data subject can contact the ICO if they are not satisfied.

## What if the Data Subject complains to the ICO regarding a SAR?

There may be occasions where an individual complains to the ICO, so you should always be ready to justify any decisions made. If an individual complains, you will receive an email from an ICO caseworker detailing the complaint and asking you to comment. Typically you will be given 14 days to respond. Your response should include:

- A description of the personal data that you have disclosed (e.g. list volume of emails and documents and number of call recordings).
- The date of the response and the method you used to send it.
- Details of any data not disclosed and the reason why not (e.g. use of an exemption or because it contains personal data belonging to another individual).
- Answers to any specific questions.

### Top Tips

1. Be Prepared.
2. Have a clear policy for dealing with SARs. Draft a precedent response letter.
3. Know where you hold personal data. Check everything including email systems, telephone/meeting note recordings, any client management system used, paper files. Remember: generally the data subject will know what they are looking for.
4. Check information before disclosing to make sure it does not contain the personal data of another data subject.
5. Ensure all staff: (i) can recognise a SAR and (ii) know that anything they write in emails/correspondence/file notes is potentially disclosable.
6. Consider exemptions to disclosure.
7. Keep a central record of all SARs and how they are dealt with/any issues arising.