LOCKTON®

DATA PROTECTION: SUBJECT ACCESS REQUESTS

2025

Contents

Introduction

The right of access is one of the eight rights set out in the UK General Data Protection Regulation (UK GDPR) under Article 15.

The right is exercised by an individual (referred to as a "data subject") making a subject access request to a data controller – this is usually referred to as a SAR (Subject Access Request) or DSAR (Data Subject Access Request).

This Guide provides an overview of the right of access and guidance on how to deal with a SAR if you receive one.

THE LEGISLATIVE AND REGULATORY REQUIREMENTS

The UK data protection regime is comprised of the UK GDPR as supplemented/tailored by the Data Protection Act 2018 (DPA).

Under data protection law individuals have the right to request:

- Access to the personal information that you hold about them.
- Confirmation that their data is being processed, and.
- To receive other supplementary information, as detailed in the UK GDPR.

Paragraph 2.1(a) of the SRA Code of Conduct for Firms (COCF) requires firms to have effective governance structures, arrangements, systems and controls in place to ensure that they comply with all the SRA's regulatory arrangements, as well as with other regulatory and legislative requirements which apply to law firms.

You will therefore need to make sure that are ready to deal with a SAR if you receive one.

WHAT IS A SUBJECT ACCESS REQUEST (SAR)?

A SAR is when an individual (known as a data subject) exercises their right of access to personal data under the UK GDPR (see further below).

SARs have the potential to have a significant impact on a business in terms of the time spent in processing such requests and can be extremely disruptive, particularly if you hold a large amount of data on the data subject. For that reason, it is important that data controllers have a clear process in place to deal with them if received.

The right is subject to the rights of third parties and the satisfaction of a number of criteria outlined in the UK GDPR. Individuals can make SARs verbally or in writing, including via social media, a third party can also make a SAR on behalf of another person.

If you fail to comply with the provisions of the UK GDPR when you respond to a SAR, this may render you liable to prosecution as well as giving rise to potentially significant fines. You should respond without delay and within one month of receipt of the request.

WHAT IS PERSONAL DATA

An individual is only entitled to personal information that relates to them, ie their personal data, which the data controller, in this case the law firm, holds in electronic form or in a so-called "relevant filing system".

The individual must be able to be identified or be identifiable either directly or indirectly from one or more identifiers or from factors specific to the individual.

Common "identifiers" include names, identification numbers, location data, and online identifiers (eg internet protocol (IP) addresses and cookie identifiers).

The Information Commissioner's Office (ICO) has issued guidance that suggests in most cases, paper records would amount to a "relevant filing system" for the purposes of data protection law if they are held in a sufficiently systematic and structured way.

If paper records are held in no particular order, ie they are unstructured, and not intended to be part of a filing system, you do not need to provide this information.

It is important to note that the fact an individual may be named in a document does not necessarily mean that the entire document is that individual's personal data. For information to be considered as personal data it should be biographical in a significant sense and the individual making the request ought to be the focus of the information.

WHAT FORM DOES THE SAR HAVE TO TAKE?

The UK GDPR does not state how a SAR needs to be made or the form it must take.

Whilst we would generally expect a SAR to be made in writing, it is important to let your staff know that a SARs can be received in any number of ways including:

- by post.
- by fax.
- by email.
- via a social media account, such as Facebook or Twitter.
- using a website contact form.

Verbal requests can also be made but you are not obliged to respond to a verbal request unless and until you are satisfied as to the identity of the person making the request.

The person responsible for data protection at your firm (who may be your Data Protection Officer, the DPO, if you have one) should be responsible for determining whether the request is in fact a valid SAR.

It is important that staff receive training on the various ways in which a SAR may be made so that they know how to identify a SAR, and that, given the short statutory timeframe you have to deal with it, they understand the importance of bringing it to the attention of your DPO without delay.

THE RIGHT OF ACCESS

The right of access is intended to help individuals to understand how and why you are using their data and allows them to check you are doing it lawfully.

Individuals are only entitled to their own personal data – not to information relating to other people (unless the information is also about them or they are acting on behalf of someone).

The supplementary Information

In addition to a copy of their personal data, you are required to provide the following supplementary information, which you should provide when you send the personal data:

- the purposes for which their personal data is being processed.
- the categories of personal data concerned.
- the recipients or categories of recipient you disclose or will disclose the personal data to.
- your retention period for storing the personal data or, if you cannot provide this, your criteria for determining how long you will store it.
- the existence of their right to request rectification, erasure or restriction of processing or to object to such processing.
- the right to lodge a complaint with the Information Commissioner's Office (ICO).
- information about the source of the data, if it was not obtained directly from the individual.
- the existence of any automated decision-making (including profiling); and.
- the safeguards you provide if you transfer personal data outside of the UK.

Most firms will already be providing most of this information in their Privacy Notice. However, it is good practice to also provide this when you respond to the SAR.

WHAT TO DO WHEN A SAR IS RECEIVED

If you receive a subject access request you should do several things:

i. Ensure the request is logged and complied with promptly

Individuals don't have to expressly state that they are making a subject access request or make reference to the UK GDPR or DPA for their request to be valid.

It's therefore important that you ensure that all of your staff receive training on data protection compliance so they can recognise a SAR when it's made and know what to do.

They will need to pass it to the person responsible at your firm for dealing SARs immediately, so that the request can be dealt with promptly and within the statutory 30-day deadline – the clock starts ticking as soon as the request is received.

You may extend the time limit by a further two months if the request is complex or if you receive a number of requests from the individual.

ii. Check that there is sufficient information to respond to the request

You are not required to respond to a request until you have all of the information that you reasonably require to enable you to respond.

If the SAR is not clear, you are entitled to go back to the individual for more information.

However, you should not use this as an excuse to delay a response or gain extra time to deal with it and you must avoid appearing obstructive.

The 30-day time limit for responding to the request will not start until this additional information, if requested, has been provided.

You should perform a reasonable search for the requested information.

iii. Can you charge a fee for dealing with a SARs?

In almost all circumstances the information requested must be provided free of charge to the data subject.

You can only charge a reasonable fee where you consider the request to be "manifestly unfounded or excessive". In these cases, the time limit will not begin until payment of the fee has been made. You cannot use this as a tactic to delay your response – you have to be able to justify your decision.

iv. Checking the identity of the person making the request

If you are unsure of the identity of the person making the request and whether they are entitled to the information, you can ask them to provide evidence of their identity.

If an individual is writing on behalf of a spouse or is a legal representative acting on behalf of their client, you should not assume that the requestor has authority to act on behalf of the client/individual and you should ask for written evidence of authority.

Authority could be a written statement of authority or a general power of attorney.

Alternatively, telephone the individual and based on the information that you hold about them, you should ask two or three reasonable questions to allow you to confirm their identity. The DPO should keep a record of what measures are taken to verify identity.

v. Carry out a search for the information requested

Provided you have enough information, you should start your search for relevant personal data as soon as possible.

The DPO will generally be responsible for organising this search, although you may decide to appoint someone else to deal with this depending on the size of the project and the DPP's knowledge of the business area.

You should bear in mind that the person making the SAR is likely to know what they are looking for – and they may assist you by listing exactly what they require. However, they may make a general request – in which case you will have to provide all the personal data you hold, subject to any exemptions that are available to you.

You will need to consider and decide where the personal data is likely to be held – it may be in any number of places. You will need to search central filing systems, electronic and manual records (subject to the "relevant filing system" criteria mentioned above), HR records, shared drives, the firm's intranet, if you have one, and/or private filing systems of particular individuals.

You may also need to ask colleagues to search through their personal drives and email accounts for personal data and ask whether they are aware of any areas that may hold information about the person making the SAR.

You do not need to look through unstructured personal data unless a specific piece of information has been requested and its location has been identified.

At this point, the DPO should consider whether he/she considers that the cost of supplying the data is likely to be excessive and whether a fee can be charged in line with the DPA. This is likely to only be in exceptional circumstances.

You will also need to consider whether any data processors that you use are holding personal data (for example, if you use outsourced payroll providers) and if so, contact them as soon as possible. Your contract with them should oblige them to provide you with all necessary, reasonable assistance to deal with the SAR.

Archived, but not deleted, data should also be searched provided it constitutes a "relevant filing system".

EXEMPTIONS

The DPA and UK GDPR lists a number of exemptions to the obligation to disclose personal data.

You should not routinely rely on exemptions or apply them in a blanket fashion and should consider each one on a case-by-case basis.

In line with the accountability principle, you should justify and document your reasons for relying on an exemption so you can demonstrate your compliance.

We have summarised below what we believe are likely to be the most relevant or useful exemptions:

The Exemption	Information that may be exempted
Confidential references	References given or received by the data controller (ie the law firm) that are connected to actual or prospective education, training or employment of the data subject.
Management forecasts	Data used for forecasting or planning, but only to the extent that disclosure would be likely to prejudice your ability to conduct business.
Negotiations with the individual	Information which relates to ongoing negotiations between the data controller and the person making the SAR, but only where disclosure would prejudice those negotiations.
Prevention or detection of crime	Any information if its release would prejudice: • the prevention or detection of crime. • the apprehension or prosecution of offenders; or. • the assessment or collection of any tax or duty or of any imposition of a similar nature.
Repeat requests	Identical or similar requests do not need to be responded to unless a reasonable time has elapsed since the previous request or there is a reasonable circumstance.
Manifestly unfounded or excessive	Data controllers can refuse to respond to these types of requests but will need to be able to provide evidence of how the conclusion was reached that the request is manifestly unfounded or excessive.
Legal Professional Privilege	Any information to which a claim to legal professional privilege could be maintained in legal proceedings or in respect of which a duty of confidentiality is owed by the data controller to a client.
Right to withhold	Data controllers can withhold personal data, in whole or part, if disclosing it would adversely affect the rights and freedoms of others.
Private Records	If a record was created by a member of staff whilst acting in a private, rather than an official capacity, only exceptional circumstances would justify its disclosure without their consent. If they are not prepared to disclose the record, you should not disclose it. Note: we would generally expect a law firm's IT policy to only allow limited personal use of computing facilities and you should take this into account.
Third Party information/ Protection of the rights of others	You cannot refuse to provide access to personal data just because the data refers to a third party. Instead, you must undertake a 'balancing act' to ensure the privacy rights of the individual requesting the data and the third party included in the data are respected. Where the data includes third party information, it may be possible to: • anonymise the data relating to the third party. • seek consent from the third party; or. • decide if the disclosure is reasonable, bearing in mind any duty of confidentiality owed to the third party, any statutory requirements as well as the type of information to be provided.
Disproportionate effort	Data controllers can refuse to provide information where to do so is impossible or would involve disproportionate effort. You may take difficulties throughout the process (from finding, analysing and providing the data) into account, but must be able to show that you have taken all reasonable steps to comply with the request. It is worth noting that the ICO code of practice on SARs states that data controllers "should be prepared to make extensive efforts to find and retrieve the requested information."

If you do decide to rely on an exemption, the DPP will need to make a record of the rationale for applying the exemption, as they may be asked to justify their decision at a later date.

PROVIDING THE PERSONAL DATA

Once all of the personal data that can be sent in response to a SAR has been identified, we strongly recommend that one final review of the information is done by the DPO or another appropriate person.

This is to offset the risks often discovered in collating information. Whilst on the face of it, information that has been collected may appear unrestricted in its nature, once it is aggregated with other information there is a risk that additional information could be disclosed or at least interpreted. This needs to be taken into consideration before the final response is made.

You should also remember and take care to:

- Remove any duplicate records - for example, if there has been an email exchange with some work colleagues, you should only print the last email in the exchange if copies of all the other emails are part of the last email.
- Double-check that the information does relate to the person concerned and not to someone else with the same or very similar name.

It is important to note that the individual is entitled to a copy of their personal data and not a copy of the documents that contain their personal data, so you can provide the personal data in a separate document should you wish.

The UK GDPR requires that you disclose the personal data disclosed in an intelligible form. For example, if codes have been used, a key to those codes should be provided so the individual can understand the information, but there is no requirement to make the data legible or even understood by the recipient, for example, translated in their preferred language.

THE SUPPLEMENTARY INFORMATION

Do not forget to provide the supplementary information referred to above.

A formal response letter should also accompany any information that you disclose and include this supplementary information.

It is good practice to prepare a standard form of response for use with SARs as this will save you time in the long run.

LOGGING SARS AND RESPONSES

Your firm's DPO should record and track the progress of each SAR so that you do not miss the deadline for response.

We recommend that you record the following information on the file:

- Copies of all correspondence between the data subject and the DPO or any other party.
- A file note of any telephone conversation used to verify the identity of the data subject.
- A note of the DPO's decisions and how those decisions were reached.
- Copies of the information sent to the data subject - for example, if any the information was anonymised or redacted, keep a copy of the anonymised or redacted version that was sent. These records should be kept and then securely destroyed in accordance with your firm's Data Retention Policy.

Useful resources

- ICO Guidance:
- UK GDPR guidance and resources | ICO