Subject access requests – FAQs

Under the UK General Data Protection Regulation (UK GDPR), individuals have a right to request access to their personal data from SGBs who are controllers of that personal data – such requests are often referred to as "subject access requests". All individuals within SGBs should be able to identify a subject access request to ensure that it is responded to in accordance with the SGB's legal requirements under the UK GDPR.

This briefing aims to answer some of the most commonly asked questions from SGBs when they receive a subject access request (SAR).

How do we recognise a request?

A SAR from an individual may be made in writing or verbally. The Information Commissioner Officer's (ICO's) website includes an example request and this is often the version that we see SGBs receiving from individuals, most commonly via email.

However, individuals do not need to expressly refer to the UK GDPR, subject access request or personal data. Often we see individuals incorrectly referring to FOI or the Freedom of Information (Scotland) Act 2002. Although SGBs are not subject to the legal requirements to disclose information under this Act, if an individual is wanting to access their own personal data then SGBs should not dismiss the request.

Any request seeking access to or a copy of their own personal data will need to be treated by SGBs as a SAR under the UK GDPR.

How long do we have to comply?

The timescale for responding to a SAR is "without undue delay and at the latest within one month of receipt". This period starts as soon as anyone within or acting on behalf of an SGB (for example, a board member) receives the SAR so it is important that it gets to the person who will deal with it as soon as possible.

The time limit is calculated from the day the SAR is received (or, if clarification has been sought, from the day clarification has been provided) whether or not this is a working day, until the corresponding calendar day in the next month.

If the corresponding day is not a working day, then the response is due on the next working day after the corresponding day. If the corresponding day does not exist (for example, 31 November) then the time limit expires on the last day of the month (for example, 30 November).

Can we refuse a request?

A SAR can be refused in full if it is manifestly unfounded or manifestly excessive. In our experience, it is quite difficult to demonstrate this and there is always the risk that refusing a SAR in full would lead the individual to raise a complaint with the ICO and the SGB would need to provide evidence to satisfy the ICO that it was right to refuse the SAR in full.

Manifestly unfounded requests include where the individual has no intention to exercise their SAR right – for example, the offer to withdraw it in return for a benefit – or it is malicious in intent and is only being used to harass the SGB with no real purpose. Most often we see individuals making SARs to SGBs in the context of complaints or disciplinary matters.

While the SGB may consider that the individual has only made the SAR to cause nuisance, if the individual has genuinely requested information to help them with their complaint or during a disciplinary investigation, then it would, in our view, be difficult to justify refusing the SAR in full to the ICO. There are certain exemptions that can be applied in such circumstances (see further details below) and so it may be more prudent for the SGB to comply with the SAR but withhold certain information if an exemption applies.

Manifestly excessive is where a SAR is clearly or obviously unreasonable – this involves SGBs considering whether a request is proportionate, taking into account the burden or costs involved in dealing with the SAR.

It is not just whether the individual has requested a large amount of information as all of the circumstances of the SAR must be considered. Where an individual has requested access to all of their personal data and this constitutes a large amount if, for example, that individual has been involved with the sport for 15 years, then the SGB may consider whether to seek clarification on what the individual is actually seeking.

There is legislation currently in draft form introducing provisions to refuse a SAR where it is vexatious. Please keep an eye on the hub for updates on when the new legislation comes into force and if this provision is adopted.

Can we charge for responding to a request?

The UK GDPR provides that SGBs can only charge a 'reasonable fee' to cover your administrative costs of complying with a SAR where such request is manifestly unfounded or excessive. The only other time a fee can be charged is if an SGB has provided an individual with access to their personal data and they request further copies. Again, such fee is only to cover the SGB's administrative costs.

How do we search for personal data?

Guidance from the ICO provides that SGBs should make "reasonable efforts to find and retrieve the requested information" as there is a high expectation on SGBs to provide information in response to a SAR under the UK GDPR.

Where your IT systems permit global searches of all files and emails, this facility should be used to search all information held by the SGB. Where you need to rely on individual searches, it is important to provide clear guidance to individuals on what search terms should be used to locate all relevant information – for example, the individual's full name, initials and any references to position, job title or other term used to refer to them.

SGBs with volunteers may need to ask volunteers to search their personal files, particularly if they have been processing the requestor's personal data on behalf of the SGB. We would always recommend that board members and other volunteers regularly engaged by SGBs are given SGB email addresses to ensure that there is a clear distinction between information used for SGB purposes and other personal or business purposes.

If the individual raises a complaint with the ICO regarding how an SGB has handled their SAR, one of the questions that the ICO may ask is how the SGB searched for information so it is important to keep an audit trail of all searches to demonstrate that the SGB complied with the terms of the UK GDPR.

Information is also 'held' by an SGB if it is included in your back-up files or deleted items and so these will need to be searched as well, provided it is reasonable to do so.

When searching for information it is important to consider what actually constitutes the requestor's personal data. The only information that an individual is entitled to receive under a SAR is their personal data, which means that the information must relate to them and they can be directly or indirectly identified from it.

Take emails, for example, an individual may have sent and received a number of emails but the content of the email does not relate to them or include their personal data. SGBs are not required to provide such emails in response to a SAR – although the ICO suggests that you confirm in your response that you have identified X number of emails that they have sent or received. It is only emails where the body of the email relates to the requestor and, therefore, contains their personal data, that you would need to provide access to under the UK GDPR.

What can we withhold?

There are a number of exemptions to the obligations to disclose information under SAR, which are contained in the Data Protection Act 2018. The main one is where the information includes the personal

data of other individuals. If information within the scope of a SAR includes third party personal data, SGBs need to consider the following:

- Has the other individual provided consent to the disclosure of their personal?

There is no obligation on SGBs to ask the third parties for consent as it may not always be appropriate to do so – for example, the third party is a former employee or the third party has made a complaint against the requestor. There may also be situations where it would be inappropriate for an SGB to notify the third party that the requestor has submitted a SAR by asking for their consent to disclose personal data.

- Is it reasonable to disclose without consent?

If the third party has not consented to the disclosure of their personal data, SGBs then need to consider if it would be reasonable to disclose without consent. SGBs must take into account all of the relevant circumstances, which includes the type of information; any duty of confidentiality owed to the third party; any steps to get consent; whether the third party can consent; and any refusal of consent.

In our experience, where the requestor has already seen the third party personal data – for example, the requestor has received an email from an SGB employee – it would be reasonable to disclose that third party personal data. One reason for this is that even if the requestor was given a redacted version of the email, they would be able to identify the third party as they have had already seen the full version. This would be the same for information that is generally available to the public.

Some of the other exemptions that may be relevant for SGBs are:

1. Where personal data is processed for management forecasting or planning about a business or other activity if disclosure would prejudice that business or activity;

2. Where personal data is a record of the SGB's intentions in negotiations with an individual if disclosure would be likely to prejudice those negotiations; and

3. Where the personal data is in confidential references either given or received by the SGB.

Each exemption needs to be applied on a case by case basis, with appropriate advice if required, and a response still needs to be provided to the requestor with the exempt information either redacted or withheld in full and the SAR cover letter confirming that an exemption has been applied.

How do we disclose the requested personal data?

The right of subject access under the GDPR entitles an individual to obtain access to their personal data, rather than a right to see copies of documents. Accordingly, SGBs can decide whether to provide access to personal data under a SAR in the form of transcripts or sections of documents, or by providing a copy of the actual documents.

Personal data must be provided in a "commonly used electronic format" under the GDPR, although there is no specific definition of this.

However, the format should be easily accessible by the requestor and provided in a secure manner.

What other information needs to be provided?

In addition to providing individuals with access to their personal data, SGBs must confirm the following under a SAR:

- the purposes of processing the personal data;
- the categories of personal data;
- recipients of the personal data;
- applicable retention periods;
- if personal data has not been collected from the personal data, details of the relevant source;
- the existence of the right to rectify or erase personal data and restrict the processing of personal data or object to such processing;
- the right to lodge a complaint with the ICO; and
- if there is any automated decision-making regarding the personal data.

We would recommend that SGBs prepare a template cover letter, which includes the above information, and updates this for each SAR response.

Do you need to comply with a SAR if the worker is going through a tribunal, grievance or conduct in sport hearing?

Yes. People have the right to obtain a copy of their personal information from you. You cannot simply refuse to comply because the worker is undergoing a grievance, tribunal process or conduct in sport hearing, and you believe they intend to use their personal information to obtain information for potential litigation. If you believe it isn't appropriate to disclose the relevant information, you must demonstrate what exemption you are using and why. It may be that there are other exemptions which can be relied upon, but this should be considered on a case by case basis. It is important to note that whilst there may be separate rules for disclosing information in the course of a tribunal or hearing, you must comply with a SAR. This applies even if there may be some cross-over in the information supplied.

However, even if you have already disclosed the information through another statutory process, such as in employment tribunal proceedings, this does not mean you can refuse to comply with a SAR. Documents disclosed for the purposes of the litigation may not contain all the worker's personal information. Alternatively, the worker may have only been allowed to view the information rather than receive a copy. In this instance, you must review the request and, where possible, provide them with a copy of their information. You may also hold other personal information that was either not required to be disclosed at the time of the tribunal or did not exist at the time. You could potentially disclose this information under a SAR, particularly if you did not disclose it during the tribunal proceedings.

You should also bear in mind that the information disclosed during the tribunal proceedings is given to the worker's legal representative and not to the worker. You cannot assume that the worker can access any or all the information, just because you have provided it to their lawyer. They may also have changed their legal representative during the case. You should carefully consider the circumstances of the request and must ensure you provide all the worker's personal information that they're entitled to.

Do we have to include searches across social media?

Yes. If the SGB uses social media platforms such as Facebook, WhatsApp, Twitter and chat channels on Microsoft Teams for business purposes, then you are the controller for the information processed on those pages. The UK GDPR applies to any social media activity carried out in a commercial or professional context. If you receive a SAR, you must search these platforms for any personal information if it falls within scope. This would also extend to Microsoft Teams and Whatsapp. You should also consider social media posts supplied to you by others as potentially in scope. For example, if a worker submits a copy of posts made by a colleague criticising their manager in a WhatsApp group.

Get in touch

SGBs can access the **sport**scotland legal expert resource helpline by email at **sport**scotlandinfo@harpermacleod.co.uk or by calling 0141 227 9333.