VIBRANT NATION

Guide to Subject Access Requests

VIBRANT NATION

What is a SAR?

Most of us have heard about the GDPR. One of the rights that an individual has under the new regulation is access to their personal data. This means that they can write to your organisation and ask you for a copy of their information and you also need to tell them how you use it.

This is a Subject Access Request (SAR). Sometimes it is called a Data Subject Access Request (DSAR).

You MUST comply with a SAR; it is not optional, and you must also return the information to the person who requested it within one month of the request or one month after you have received proof of their identity.

This is not very much time to do this, especially if you have a lot of personal information to look through.

You are not allowed to charge a fee for doing this, unless you have been repeatedly asked for information that you have already provided.

Be prepared – know where your personal data is

Do you know where personal information is stored and used in your organisation? It will make your job much easier when presented with a subject access request if you already know where to look for a person's information. Keep a record of everywhere personal information is used.

It is much easier to do the searching for personal information if you know where to look! Go through your processes and make a record, maybe on a spreadsheet, of where personal information is used. Some things, like e-mail, are obvious. Sometimes personal information is processed by people as part of their function in the organisation and they may keep this themselves.

Talk to your staff and volunteers – learn where personal information is in the organisation ahead of any SAR request that may arise. You'll be glad you did!

SARs from parents or children

There is a lot of confusion about the rights of children (i.e. under 13 years of age in the UK) to access their personal information under the GDPR. There is also much confusion about the right of a parent or legal guardian to access the personal data of a child. There is also a slight difference between England and Wales, and Scotland.

It is a question of competence. Children have the same rights to access to their personal data under the GDPR as an adult. If a child is mature enough to request their data and to understand what they are requesting, then it is reasonable to consider they are competent to make the request. The second consideration must always then be if fulfilling the request is in the best interests of the child.

In Scotland it is presumed that any child over the age of 12 is competent to make such a request.

There is an equivalent issue if a parent requests a child's personal data. If the child is able, they should give consent for this and in any event, it must be in the best interests of the child for this information to be given to a parent or guardian.

If the situation is borderline, the ICO have suggested the following points to assist in decision making:

- where possible, the child's level of maturity and their ability to make decisions like this;
- the nature of the personal data;
- any court orders relating to parental access or responsibility that may apply;
- any duty of confidence owed to the child or young person;
- any consequences of allowing those with parental responsibility access to exercise the child's rights. This is particularly important if there have been allegations of abuse or ill treatment;
- any detriment to the child or young person if individuals with parental responsibility cannot access this information; and
- any views the child or young person has on whether their parents should have access to information about them.

What does a SAR look like?

There is no set form or wording for someone to use to make a SAR to an organisation. A SAR can be made via an e-mail, a letter or even over the phone so how do you know if you have had a request?

As a rule of thumb, if someone asks for a copy of their personal information, then they are making a SAR even if they don't use words like *subject access*, *GDPR* or *data protection*. If you are at all unsure, then it is a simple matter of asking the requestor if they are asking for their information under the new GDPR rules.

Always remember that a SAR is only about the requester's personal information. It is not a way to get hold of any other information about your organisation, or your staff or volunteers.

Communicate the request

You will need to inform all the staff that handle or create personal information that a SAR request has been received. Make sure that you have given everyone clear instructions on what data is required. You may only need to supply information that has been collected for a specific purpose or that has occurred within certain dates.

It is a good idea to provide everyone who needs to respond to the request an e-mail to send information that is found to. This will ensure that all the information ends up in the right place to be checked and collated.

Ensure that all staff have received the information sheet on responding to a SAR. It would be a good idea to send an e-mail from the address that replies should be sent to and attach a copy of the information sheet.

Collation of information should be started straight away. If you need identification from the data subject do not wait before starting to search for information unless you are sure the request is a false one. Remind staff that all information must be returned to the coordinator and NOT sent to the subject directly. Take care when dealing with e-mails.

Identify the person making the request

It is important that you do not request an excessive amount of ID from someone who has made an access request. Of course, if the personal information you process is sensitive then you must make a proportional attempt to ensure the applicant is who they say they are.

It is very important that you are sure that the person who has made the request is the actual person that the personal information is about. The request may be made by someone acting on their behalf, in which case you should ask to see a letter of authority as well as ID for the data subject.

Where the personal information is very low risk, maybe a name and e-mail for example, then if you have received the request from the e-mail you have on file for them, this is a good indication that the request is legitimate. A quick reply confirming the request will validate this.

Where information is more sensitive, then a copy of the subject's driving licence or passport is a good from of ID. You need to explain what you will do with this ID – it is processing of personal data after all. Ensure that you destroy the ID documents once the request has been fulfilled.

Calculating the SAR response date

The response date is the date, one month forward, from the date you received the request or received the proof of identity if you have requested it (but don't delay asking for proof of ID to give yourself more time). If the response date falls on a weekend or a bank holiday, then it is the next working day after that. Any request made in February will give you 28 days and this is a good number to use. Always aim for completing within 28 days and you should always be within time.

Safeguarding information

This section will not apply in Scotland. Scotland has its own rules.

There is an exemption in the Data Protection Act 2018 from disclosing safeguarding data about a child under the age of 18 or an older person that does not have capacity to manage their own affairs. It is outlined in Schedule 3 Part 5. You are not obliged to confirm the fact that you are processing safeguarding information nor are you obliged to provide the data subject or their representative any access to such data. Additionally, you are not required to notify the data subject if safeguarding data concerning them is transferred internationally.

Withholding under this exemption is permitted if releasing the information would not be in the best interests of the data subject. This exemption also applies to the legal guardian of the child as well.

Don't get a SAR mixed up with a request for safeguarding information from another authority or organisation. The provision of safeguarding information to the police or social services for example, is not to do with a SAR and is permitted. Always seek advice if you are not sure.

Health information

Under the Data Protection Act 2018 access to health data by the data subject is RESTRICTED. You are NOT ALLOWED to disclose health information without first having consulted a health professional who must assess the data and ensure that no harm will come to the subject if they were to see their health information.

If you are a health professional, you must make sure that the serious harm test is conducted and not met prior to the release of any information.

ALWAYS get advice when it comes to health data and remember to get authority from a medical professional before releasing health information under a SAR. If you are in any doubt, then DO NOT release the information.

DO NOTS when you have received a SAR

Do not ignore it! You need to begin the process as soon as you receive the request. Time will pass quickly and may run out, especially if you put off dealing with it.

Do not panic. Sometimes there may be a fear of causing a problem by responding to a request fully. If the request is made by someone with a complaint, this can be especially worrying. Always get some advice, quickly, if you feel that your responding to the request is going to make a situation worse.

Do not delay asking for proof of ID. You should ask for proof of ID as soon as you have determined what proof you need. It is unreasonable to delay this too long. It may well end up as a complaint to the ICO if you do this.

Do not be tempted to charge for fulfilling the request even if there is a lot of information. There are very few circumstances where you would be allowed to charge a fee and generally this only when you get repeated requests for the same information. If this is happening, get some advice before you mention fees to the requester.

Do not be tempted to alter any information or to delete anything. You are not allowed to change the data once you have received a request under the GDPR. Doing so will most likely get you into hot water and always remember that often the requester knows what information you have.

Do not try and persuade the requester to withdraw the access request. You might find, however, that they might use this as a bargaining point if you are engaged in discussing any kind of settlement. Always get advice if this arises as it can make things tricky.

Do not be afraid to ask the requester to be more precise with the data they are looking for. Often, they will tell you what they want, and this will make your job easier. However, if they want everything you have, then this is what you must provide.

Remember that altering or deleting personal information after a request has been made is a CRIMINAL offense. Communicate this to your staff with a suitable warning about being tempted.

Collating information

Set up a secure folder on your server or a desktop machine to store all the information ready for inspection and assessment. Try and get all the responses from the organisation as PDF files. You might wish to use subfolders to categorise the information sources e.g. e-mails, HR etc. Create a log in the folder, possibly use a spreadsheet, to note where a piece of information came from, why it is used in the organisation and who it has been sent to and along with any other useful information. Tag each PDF with an item number as you enter them into the log. This will make it easier to keep track of each item.

Go through each piece of information that is collated and decide:

- Is it about the requester?
- Is there anyone else's personal information in it?
- Should anything be redacted
- Should this be withheld
- Is this duplicated information

Use columns in the spreadsheet to flag any items that fit the criteria. You could think about colour coding each row to give a visual clue to how far through the process each item is – maybe green for ready to send, amber for attention, red for withholding etc. Devise a scheme that works best for you and your team.

Remember to ensure that this store of data is VERY SECURE and that it is not generally accessible to people in the organisation. You may be gathering sensitive information together in one place and you must make sure that it is secure and protected.

Third party personal information

There is a common misperception that you should never disclose information that also concerns a third party. There is a stipulation that any information you release should not *adversely* affect the rights of a third party but that does not mean that you never give the information out.

If the third party is a member of staff, then it is reasonable that their name or job role be included in a response to a SAR as they cannot reasonably expect the fact of their job or employment with the organisation to be private. You might, however, redact their e-mail address if this is not generally known or is a personal one.

The existence of third-party information pertaining to children and vulnerable persons should always be redacted. If much of the information concerns the child and has little to do with the requester beyond a mention, then it should be withheld.

Likewise, information concerning adults should be redacted from the response unless you can get consent from the third party and they allow the information to be released. This may be relevant in the case of a volunteer for example.

There is some legal case-law that sets out the need to balance the rights of the requester against the rights of the third party. It is worth considering this and documenting the reason for your decision on the log that you are keeping. If there is any doubt, seek advice.

Redacting information

To redact information, use a software tool to do this in a copy of the PDF and name it 'redacted'. Adobe Acrobat Pro has this function and there are other programs available. This puts a black bar *in place* of the information (not over it). Follow the instructions for your software.

Any documents that are paper based should be scanned to a PDF format and then redacted where needed. This will also make collation of the response easier to manage as it will all be electronically held in the one location.

Never send MS Word documents that you have tried to redact. This is extremely hard to do properly and can often be reversed thus revealing the redacted information. Save Word documents as a PDF and then redact as required.

Withholding information

There are several cases where you are able to withhold information from a response to a subject access request. Under the second two situations you do not even have to acknowledge the information exists and it is recommended that you do not do so. We will look at the three main reasons that you would withhold information for.

Only a passing mention.

To come under the request, the information concerned must relate to the requester and not just be a mere mention of their name. Here are some examples.

Not personal information: When I arrived, I said "good morning" to John Doe.
Personal information: When I arrived, I said "Good morning" to Jane Doe, Jane passed out on the floor and was then sick.
Not personal information: I saw John Smith today.
Personal information: I saw John Smith at our board meeting today, he is a trustee.

You need to be careful when considering this particular aspect. If there is nothing of any consequence in the information and it does not infringe the rights of others, then it is better to disclose it.

During a negotiation

If any information would interfere with your ability to negotiate with the data subject in an ongoing situation then you may withhold it. You need to be very careful that it is directly concerning your position and the negotiation must be active at the time that the response is made. If the negotiation stops, all the information in this category should then be provided.

It is a good idea to get advice if there are negotiations going on and a SAR is received.

Legal Privilege

Where you have sought legal advice from a legal professional, you may be able to withhold information based on legal advice privilege. Any documents that contain personal information of the requester that have been prepared for litigation, maybe an employment tribunal for example, can be withheld under litigation privilege.

Always seek advice about using legal privilege to withhold information as it doesn't always apply to everything between the organisation and a legal advisor. It can be quite complex to get right.

CCTV Footage

If you use CCTV or any other form of video surveillance, you may be asked to provide footage or still images regarding and individual as part of a SAR.

This is probably going to be the most time-consuming part of any request as you will need to review camera footage for the period in question. Always try and get the requester to specify dates and times that they may have been at a premises that will have had CCTV capture, this will narrow down your search.

Ask the requester for a passport-style photograph of themselves that is representative of how they looked at the time they are requesting footage from. Also try and get them to describe their clothing. These will assist in searching for images.

Depending on how long you retain CCTV recordings for, you will likely have many hours of recordings to go through. Start with the entry camera and find the requester coming on to the premises. You can then 'follow' the subject around from camera to camera using the timestamp to quickly zero in on the right section of the recordings. Make notes of the camera number and time for each section.

You only need to provide footage where the subject is clearly identifiable. This may be as a result of an earlier section of footage and continue to relate to them even when their face is not visible. Try and find as much coverage of the subject as you can.

Extract all the footage from the system and place it in the folder with the rest of the information you have collated. You will need to obfuscate (blur or pixelate) any other clear faces in any of the footage. There is software that can do this or alternatively, there are companies that can undertake this work for you.

If you have been asked for still images, then choose frames from the footage where the requester's face is clearly visible and take a 'grab' or screen capture of the frame. You can then blur or cover any other clear faces in the frame – this is within the capability of your own staff to achieve using a simple graphics program supplied with most computers.

Ensure you have the correct signage, processes and policies in place to make your CCTV system legal. Choose the shortest retention period that is practical for the footage – this will result in less work if you receive a SAR that includes material from your surveillance system.

Additional information to go with the request

As well as a copy of the personal information, you also need to provide the following information to the requester about how their personal information is used in your organisation. If you have created the inventory of the personal data described in the Be Prepared section above, this will be much easier for you to do as you can record these details in your inventory. You need to provide the following additional information:

(a) the purposes 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) where possible, 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 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; and
(h) the existence of automated decision-making, including profiling, and meaningful information about the logic involved.

This information can be summarised at the top of the response with the copies of the information attached behind. Providing this information is not optional and it must be done. Another good reason for having a data inventory.

Returning the response securely

Once all the information has been prepared to go to the requester, consideration must be given to how it is provided. Guidance from the ICO tells us that if the request is made electronically, via e-mail for example, then the information should be returned in the same way. If the requester asks for the information on paper it must be provided this way and you cannot charge a fee for doing this.

There are basically three ways to return the information to the requester depending on how it was specified. Printed material can be sent in the post and electronic information can either be sent on a memory device or transmitted over the internet. We will look at each way.

Post: Always use a strong package to contain the paperwork, especially if there is a large quantity. Securely wrap the papers and then place the pack inside a STRONG plastic mailing bag and seal it. Always use a priority tracked service to send it such as Royal Mail Special Delivery. Always request a signature on delivery.

Memory Device: Use an archive tool to compress and encrypt the files that you are returning on to the memory stick or drive. Use a strong password and send this by a different means - either via e-mail or in a separate envelope the next day. Again, use a tracked method of postage and ensure that the parcel and envelope are signed for.

File Transfer: Prepare a compressed and encrypted file in a similar way to sending on a memory device. You can then upload the file to a service we transfer or similar. If the file is quite small, you could send it via e-mail. Send the password via a different method – it would be best to send the password in the regular postal service. Don't use e-mail if you have sent either the file or the link to download the file via e-mail.

Follow up with the requester and make sure that they have been able to access the information once it has been received. Consider creating some simple instructions on how to use the password to extract the information. Give the requester as much help as you can so that they have access to their information.

If you use a cloud-based service to transfer the secured file, make sure that it is based in the UK or Europe. *WeTransfer* is based in Europe and is free to use. If the service you use is not based in Europe, you will need to ensure the data is adequately protected under the GDPR. Try and avoid this problem.

Practice makes perfect

Everything is easier if it is practiced and preparing and responding to a SAR is no different. It is a good idea to test run your whole process without telling staff what you are doing. This way you can see where there may be problems and how these can be overcome in future. Make sure that more than one person in your organisation knows how to handle a subject access request to cover for holidays and sickness. It may also be useful if you have several requests at the same time.

Make a record of where things went well and things that went wrong. Also try redacting documents to make sure you are familiar with how it is done. Finally practice encrypting the files with a password.

Getting help

If you think you need help with any aspect of responding to a SAR then the earlier you seek advice, the more likely you are to stay within the deadline.

If there are any concerns with legal privilege or when there are negotiations ongoing, then getting the right advice is important and this should not be left to the last minute.

Always remember that you can ask the requester to narrow down the material that they are looking for, most people who make a SAR have something in mind.

Talk to the CEO of your organisation as soon as you feel that you need to. They can enlist the help of the board or of external organisations to provide you with the assistance you need.

There is a lot of good advice and information available from the WSA, the NSPCC Child Protection in Sport Unit if safeguarding issues are involved, and from the ICO for general data protection advice: wsa.wales; thecpsu.org.uk; ico.org.uk.