VIBRANT NATION

Guide to Subject Access Requests

For Managers and Boards

VIBRANT NATION

Required reading

It is important that the Vibrant Nation Guide to Subject Access Requests is read before reading this document. The general guide gives a lot of important information that all senior managers and board members need to be acquainted with. If you have not read the guide yet, please do so now.

The right to access is not absolute

It is a common misconception that a data subject has an absolute right to see all the data that any organisation holds about them. This is not true. It is also a common misconception that an organisation needs to tell a data subject about every single piece of personal data that is processed regarding them even if they cannot see the content. This is also untrue.

The Data Protection Act 2018 (DPA18) gives many scenarios where the personal information that is processed by an organisation may be withheld from a subject access request (SAR) and to the extent that the existence of some personal information does not need to be confirmed or notified.

There are also some other laws in the UK that actually govern the provision of certain types of information to the data subject under a SAR – these are referenced in the DPA18 and need to be adhered to.

We will examine some scenarios in this document to illustrate how a SAR that meets some of the criteria for restriction or exemption should be approached.

Safeguarding information

The information in this section will not apply in Scotland. Scotland has its own rules. We won't cover the Scottish rules to avoid confusion.

Safeguarding information is top of the list when it comes to confusion and uncertainty when dealing with a SAR. Most important is this info-banner in the general guide:

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.

It cannot be stressed enough that a request for safeguarding information from another organisation or other authority such as the police or social services is not a subject access request.

There are three basic areas that a data subject may be involved in a safeguarding issue and be a subject in any information about the issue: The reporter of an issue; the alleged perpetrator of an issue; or the subject (victim) of an issue. When responding to a SAR, it must be remembered that priority should be given to the welfare of any victim or potential victim of a safeguarding issue. It may not be in their best interests to release information about an issue. You need to be cautious about any attempt to 'anonymise' any information as this is not always possible. Often the circumstances of a case are sufficient to identify the person concerned.

An allegation about a potential perpetrator of safeguarding issues may also quickly lead to the identity of an alleged victim. Even if the person making a SAR knows there is an allegation concerning them, remember this may well be the reason for the SAR, giving any detail about the allegation could lead to the identification of either the alleged victim or the informant. For example, even a simple date when an incident is supposed to have occurred could lead indirectly to the identification of others concerned.

When a SAR is made by someone who is suspected or indeed known to have been a victim of a safeguarding issue, there is equally a consideration as to the release of information to them, especially if they are a child or other vulnerable person.

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 data subject as well.

SARs from parents or children

Although generally anyone under the age of 18 is classed as a child, data protection law has reduced this age to anyone under 13 years of age with regards to the *giving of consent* for data processing. If you read the GDPR, it will tell you that a child for the purposes of considering consent is anyone under the age of 16. This can lead to a lot of confusion over the status of a child and it is very important to treat data protection issues separately from other issues when judging if someone is a child or not. We often say: 'for the purposes of consent under data protection law a child is anyone under the age of 13'. When it comes to responding to a SAR, it will always be a consideration of the best interests of the child and a child will be anyone under the age of 18. This consideration will come into play even if it is the legal guardian that is making the request.

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 question of the best interests of the child still remains.

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

If a guardian has made a SAR then if the child is able, they should give consent for this.

If the situation of competence of the child 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.

Always consider any safeguarding information separately, see the section on safeguarding data above.

Health information

Under the Data Protection Act 2018 Schedule 3 s.6 access to health data by the data subject is **RESTRICTED**. You are **NOT ALLOWED** to disclose health information without first having consulted an appropriate 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.

An appropriate health professional is the health professional who is currently or was most recently responsible for the diagnosis, care or treatment of the data subject in connection with the matters to which the data relates. In the case of most sports organisations this is likely to be a GP or a retained team doctor or clinician. The DPA2018 has a list of roles that qualify as a medical profession in s.204. This does NOT include physiotherapists however osteopaths and chiropractors do qualify.

The health professional must make sure that the serious harm test is conducted and not met prior to the release of any information.

Withholding information

Withholding information on the basis of negotiations or legal professional privilege is quite tricky. You should never use either of these bases for withholding purely to prevent the requestor seeing something that you don't want them to. Even material that is passed between your organisation and a legal professional does not automatically have a protected status under legal privilege. We will look at both bases.

During a negotiation

Any material that would interfere with your ability to negotiate with the data subject in an ongoing situation may be withheld. This material must directly concern your position and the negotiation must be active and ongoing at the time that the response is made. If the negotiation stops, all the information in this category should then be provided.

It Is not acceptable to start a negotiation purely for the purpose of withholding information. The negotiation must be genuine.

Legal Privilege

There are two kinds of legal privilege. These are legal advice privilege and litigation privilege. You may be able to withhold some of the material that is exchanged with a legal professional but not always all of it and not automatically.

The trickiest area is that of advice privilege. It is easier to give an example of what can and cannot be withheld. Suppose Company A approaches their solicitor and says "I don't like Joe Bloggs and I want to sack him. Not for any reason, I just don't like him. How can I get away with firing him and not get dragged into an employment tribunal?" This could not be withheld from Joe as the material would be classed as inequitable – grossly unjust and unfair.

If the company asked their solicitor "Joe Bloggs is constantly late, is bad at their job and despite having several warnings and discussions to see if there is a problem, we can no longer keep him employed. What is the correct way to dismiss him so that it is fair and legal?" This could be withheld as it is seeking advice and is reasonable in terms of wishing to be fair and wanting to comply with the law.

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 can be quite complex to get right.

General data protection compliance

The general guide lists information that needs to be supplied along with the personal information when responding to a SAR. To effectively provide this information in an accurate and timely manner, it will require the organisation to be in a good state of compliance with prevailing data protection laws.

If compliance with data protection law is neglected or not given sufficient priority or resources, it is inevitable that you may struggle with the provision of some of the required items such as the legal basis for processing etc.

It is also better if your organisation has a good knowledge of data protection principles as the data held about individuals will be less likely to cause you an issue. If staff and volunteers are cognisant that whatever is recorded about an individual may well end up being read by them, they will be more careful about how things are worded. That is not to say that any organisation should be fearful of recording important information about their staff, volunteers or participants.

Getting help

In general, the earlier you ask for help, the better the outcome will be. Don't leave seeking help to the last minute.

It is better, however, to be a bit late with a SAR than to release medical information without the required medical opinion or to release information to a child without due consideration for their best interests.

You can, in complex cases, extend the time you are allowed to respond by an additional two months. You must inform the requestor as soon as possible though, don't wait for 28 days before telling them!

Use the getting help section of the general guide.