Subject Access Request (SAR) Manual

May 2018

Introduction

The right to make a subject access request (a request for one's own personal information held by an organisation) is set out at Article 15 of the General Data Protection Regulation (GDPR).

This is very similar to the preceding right under section 7 of the Data Protection Act 1998, but there are some notable differences. These include the abolition of fees, the shortening of the deadline for dealing with a subject access request, and the right to refuse excessive requests.

There are various exemptions to the Article 15 subject access right, and these are set out in Schedules 2, 3 and 4 to the Data Protection Act 2018.

Process for responding to requests for personal information

Step one – log subject access request

You should have a process in place to log SARs and the date that they are received, and the date that identification documents were requested, and the date that they were received.

Once you are satisfied that you have verified the persons' identity, you have one calendar month to respond, unless the case is complex enough to warrant an extension (see FAQ).

The period of 1 month is based on some rather complex EU rules, but if you work to a deadline of 28 days, then you will always be within the allowed time.

Step two – request verification of identity

In order to provide personal data to a requestor you must have taken reasonable steps to verify their identity. This is to avoid inadvertently providing personal data to a third party.

You should respond to the requestor, acknowledging their request, and asking them for proof of their identity. A **template letter** is available.

The following are acceptable forms of ID:
A copy (including a photograph or scan) of the identification pages of a current passport or driving license

If the requestor cannot provide either of these, then they may instead provide TWO of the following:
A recent bank or mortgage statement or building society book
A recent utility bill

A copy of their birth certificate
Solicitors letter within the last three months confirming recent house purchase

Where the requestor is, for example, an existing staff member or a public figure, and you have a high level of confidence about their identity, then it will not be necessary to formally verify their identity.

If the requestor says that they are unable to provide verification documents due to a disability, you should ask that someone else make the request on their behalf (see FAQ).

Please note that while the 28 day clock **does** stop while you are awaiting identity verification documents, any time before you make that request counts against the 28 days. So you should have a process in place to quickly issue an acknowledgment and request for proof of identity.

Given the short time scales involved, it would be good practice to continue to process the request while you are awaiting proof of identity.

Step three – search for the personal information of the requestor

We are required to carry out an extensive, but proportionate search for the requestor's personal information. This will primarily involve looking at electronic records of emails and documents, but you may need to review paper records if you think relevant information may be held there that is not held electronically.

While the requestor is free to suggest appropriate search terms and methodologies, you are not required to comply with these. For example, a requestor may instruct you to search backups, personal email accounts, and mobile phones, and to use specific search terms, but you are not required to comply with their instructions.

You must make your own mind up about what would be an appropriate way to locate the requestor's personal information, based on carrying out an extensive but proportionate search.

Sometimes it will be clear what information the requestor is interested in, or which unit is likely to hold it. If the person responding to the SAR is confident that they have access to all of the requested data, then they can move to step four.

Otherwise, the person dealing will need to ask other staff members who they think may hold information to provide it to them so they can review it. This could be done by email.

It will generally not be proportionate or reasonable (and may qualify as an excessive request – see exemptions) **to search the entire email and/or document system of the department.** While IT are able to technically do this, it is not straightforward, and it is likely that it will identify a very large volume of material. Much of the material identified

will relate to other individuals besides the requestor, and that may involve you unnecessarily accessing a great deal of personal data that has nothing to do with the request. The output from such a search will not be in a particularly user-friendly format, and will require significant investment of staff time to manually comb through. If you are minded to ask for a general trawl of the department's systems, please consult the department's Data Protection Officer for advice before doing so.

While a general trawl is likely to be disproportionate, IT may be able to assist in carrying out more targeted searches. For example, in relation to the email accounts of staff who have left the department and who are likely to hold relevant material not otherwise available. Where this is requested, you should make sure that the material is handled carefully because it is likely to include the sensitive personal data of third parties.

It will not generally be proportionate to ask staff to search their personal email accounts unless there was some legitimate reason to believe that these were being used to conduct official business, and that they were also likely to hold personal data not held on official systems.

In cases where you consider that large volumes of personal data about a person are held, you can delay dealing with the request until the requestor specifies the activities to which their subject access request relates (see FAQ). You may also be able to refuse such a request as 'excessive' (see exemptions below).

Step four – consider exemptions

Once you have gathered together all of the relevant personal information of the data subject, you must consider whether any of it is exempt from release.

Most obviously will be any personal information that relates to a third party, such as an official's name, email address, job title. You should follow the guidance below in considering whether any information should be withheld.

Besides third party personal data, there are a range of other areas where the right of subject access is modified or restricted. These are dealt with below.

If you have identified a lot of information that the requestor clearly already has (such as emails or letters to and from them), you may wish to check if the requestor really wants all that material. Alternatively, when you reply to their request you could say that you haven't included material that they have sent or received directly, but that you will provide that if they would like it.

Step five – extract the information

Once you have identified the information that you intend to release, you can move on to extracting it.

The entitlement is to information rather than documents containing that information. But it is possible to provide original documents to a requestor, and that may well be the easiest option in relation to e.g. scanned pdfs of letters (but bear in mind that you may need to remove third party personal data).

But for personal information included, for example, in emails where substantial amounts of other information (e.g. third-party personal data) must be removed, it is likely to be preferable to extract (copy and paste) the information into a schedule. An **Example Schedule** is available.

Step six – destroy verification documents

Once you are satisfied with the requestor's identity, you no longer have any reason to retain copies of any verification documents they have sent you. Make sure that you delete them and empty your computer recycle bin.

If you have the information in paper form, place it in the confidential waste bin.

Step seven – respond to the requestor

Once you have determined what information is held and what can be released, you should write to the requestor providing any relevant documents and/or a schedule of information. A **Template Letter** is available.

This template letter makes clear that if the requestor is not satisfied they can make a complaint to the Information Commissioner, or seek redress through the courts. You should keep a copy of your reply and any information supplied in line with the normal departmental retention period.

If you are extending the time limit for responding because the request is very complex (see FAQ), you must write to the requestor within 28 days to notify them of that fact, and to provide reasons. A **Template Letter** has been provided.

If you are unable to provide a response to the requestor within 28 days, you must also write to them within 28 days to notify them of that fact, to give reasons, and to inform them of their right to complain to the ICO or seek a remedy through the courts. A **Template Letter** has been provided.

Frequently Asked Questions about SARs

What is a subject access request?

Individuals (known as 'data subjects') are entitled to ask any public body or private company for their own personal data. This entitlement extends to receiving any privacy information about how their personal information is being used, and to receive a copy of that information.

What is personal data?

'Personal data' is any information that relates to any *identified* living individual (i.e. someone who is identified in that information, such as by name). Information is also personal data if it relates to an *identifiable* living individual i.e. if the person could be identified by combining the information with other information you hold, or with information that is readily accessible (e.g. available by doing a simple web search).

So personal data will generally include an individual's name, address, phone number, date of birth, place of work, dietary preferences, opinions, opinions about them, whether they are members of a trade union, their political beliefs, ethnicity, religion, or sexuality. It also includes photographs or video of them, or biometric information such as fingerprints.

It can also include an individual's email address or job title if that sufficiently picks them out so that they can be identified (in isolation or with other information that may be held). The above list is not exhaustive.

Information about legal entities such as companies is not personal data. Also anonymised or aggregate data is not personal data (unless you also hold the keys to de-anonymise or de-aggregate it, because that makes the individuals in it *identifiable*).

It is important to remember that personal data is something that reveals something about the data subject. The contents of an email is not personal data simply because the requestor is the sender or recipient of the email. So, for example, if you receive a SAR from an ex staff member asking for all of their personal data, you are not required to provide them with every email they ever sent and received!

Do people have to say that a request is a SAR?

No. Any request for an individual's own personal information must be treated as a SAR. This is the case even if they do not mention data protection legislation, or if they attempt to make such a request using the wrong legislation (e.g. a freedom of information request).

What format must requests be in?

The only requirement is that they are in writing (unless accepting an oral request is a reasonable adjustment for a disabled person).

Can we ask requestors to narrow their request?

Not generally.

If, however, you hold large quantities of personal data on the data subject, you may request that, before the information is provided, the requestor specifies the activities to which their subject access request relates. This is very much an exception to the normal rule, and is dealt with at recital 63 of GDPR.

In the event that you do process large quantities of the data subject's personal data and they have requested all of it, you may also wish to consider refusing or levying a charge on the basis that the request is excessive (see below, and exemptions).

Can we delete information to prevent having to provide it?

No, and doing so is a criminal offence.

What information must be provided?

Information that relates to the requestor, such as their name, address, email address, personal opinions, medical information, their performance assessments, etc as applicable. (See 'what is personal data?' above.)

The information provided should be that held at the time the request was received.

You do not need to provide documents that contain personal information, or information that is incidentally included in an email or document, but which does not directly relate to the requestor.

You should also not provide information that is exempt (see below), unless it is reasonable to do so.

Where must we search?

We must look in any location where we reasonably consider that relevant personal information may be held. These may include:

(i) electronic records (or paper information that is to be entered into an electronic system). This may, if reasonable, include archived or back up information, but not deleted information that would require computer forensics to reconstruct.

(ii) any paper records that are organised in a 'filing system' i.e. paper records structured by reference to individuals, or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible (e.g. your personnel or customer file).

(iii) any paper records that are not part of a 'filing system' (see (ii)). There is, however, a cost limit for these records and these records only. Personal information in these paper records need only be supplied if the cost of locating it does not exceed the cost limit set out in the Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004. So if it would take more than 24 person hours work to locate the personal information, it is exempt on cost grounds. Multiple requests for similar information received within 60 days can be aggregated. **We are also only obliged to search for unstructured personal information in paper form if the requestor provides a description of the data sought (i.e. if they just ask for "all data" that is insufficient).**

How hard must we look?

The Information Commissioner (ICO) says: "You should be prepared to make extensive efforts to find and retrieve the requested information. Even so, you are not required to do things that would be unreasonable or disproportionate to the importance of providing subject access to the information. " (ICO SAR Code p.27, 2017)

Can someone make a request on someone else's behalf?

Yes. Someone (e.g. a solicitor) can make a request on a person's behalf, but we would need to see evidence that they were acting as the person's agent (including the normal identity verification documents).

The evidence that the person is acting as an agent for another is exempt from the requirement for immediate destruction of verification documents, but this evidence should be destroyed after a reasonable interval to allow for any disputes to be resolved (e.g. 2 years).

What fee may be charged?

No fees are generally chargeable for responding to a subject access request.

If a requestor asks that the information is provided in hard copy form, this must be provided free of charge. Where the requestor requests **additional** paper copies of the information, you may charge a reasonable fee based on administrative costs[1].

A fee may be levied where a request is deemed to be "manifestly unfounded" or "excessive"[1] (or such a request may simply be refused).

When must we respond?

[1] The Secretary of State for Culture, Media and Sport has the power to define such fees in regulations, but has not yet done so.

We have 28 days to respond to a request. That time period is suspended between the date that you request identification documents, and the date that you receive those documents.

You may reasonably extend that period by a further 56 days where necessary if the request is very complex or if the data subject has made a number of different requests for their personal data.

What format must information be provided in?

Where the data subject makes the request by electronic means, the information should be provided by electronic means where possible, unless otherwise requested by the data subject. This should be provided in a commonly used electronic form.

If a data subject requests that information is provided to them orally, we may agree to this, but we must still verify their identity, which will require the provision of electronic or paper documents.

What about repeat requests?

Where you have already responded to a request from a data subject and they make a further repeated request, you may refuse that request on the basis that it is 'excessive' (see exemptions).

In deciding whether a repeated request is 'excessive' you should take into account the period that has elapsed since the previous request, the nature of the data, the purpose for which the data are processed, the frequency with which the data are altered, and any other relevant circumstances.

What if the data is held by a contractor?

The legal responsibility to respond to subject access requests lies with the 'data controller', namely The Supreme Court.

We are legally required to ensure that all contracts with companies or bodies acting as our 'data processors' include clauses ensuring that they will assist us in responding to subject access requests.

Therefore any contractors should co-operate to assist us to respond to requests in a timely manner.

What privacy information should be provided to the requestor?

Generally privacy information about the purpose for which we are holding the data, how long it will be retained, who it is shared with etc, should have already been provided to the requestor.

This will have been provided at the time that the data was collected, or shortly after it was provided to us by a third party. There is no requirement to provide such information if the requestor already has it.

If, however, the requestor specifies that they do not have that information and they would like a copy of it, then we must provide it. In some cases this information may be in public facing privacy notices on the website. In other cases, the privacy notice may have been provided separately or is embedded in a software application. However it is formatted, we are obliged to provide that information to the requestor (along with a copy of their personal data) within 28 days.

What if the requestor complains?

You may also wish to seek the advice of the Data Protection Officer.

What if the requestor complains to the Information Commissioner?

If you are contacted by the Information Commissioner's Office in relation to a subject access complaint, please contact the Data Protection Officer.

What if the requestor takes us to court?

If you receive notification or threat of court proceedings please inform GLD and contact the Data Protection Officer.

Most relevant exemptions to the right of subject access

Where the personal data contains someone else's personal data

(see paragraph 14, part 3, schedule 2 to the Data Protection Act 2018)

Where we cannot comply with all or part of a request without disclosing information relating to another individual's personal data, then that information is exempt unless:

(i) the other individual concerned has consented to its release, or
(ii) it would be reasonable to disclose the information without the individual's consent.

When deciding whether it is reasonable to disclose the information without consent, we must have regard to all the relevant circumstances, including:

- the type of information that would be disclosed,
- any duty of confidentiality owed to the other individual,
- whether we have sought consent from the other individual
- any express refusal of consent by the other individual, and
- whether the other individual is capable of giving consent

It is worth noting that an opinion about someone can be both the personal data of the person giving the opinion, **and** the person who is the subject of the opinion.

For example, a council tenant at no.9 Acacia House contacts a local council to ask for any personal information they hold in relation to a complaint made about him by his neighbour at no.11 Acacia House (who he suspects has complained about him). Assuming such information is held, it would be impossible to respond to the request without exposing the personal data of the neighbour (i.e. that he has complained, and his opinions of his neighbour).

However, if some information could be released without identifying someone else, then it should be. For example, if the tenant at no.9 has asked for "any personal data you hold in relation to complaints made about me" then information might be able to be provided with the complainant's name and other identifying information redacted (assuming there wasn't a history of an on going dispute between these two neighbours that would allow the complainant to be identified– see paragraph 14(4)(b)(ii)).

It is important to recognise that **the decision about whether to withhold the third party data is yours**, and not the decision of any third parties. While they can consent to its release, they cannot determine that it must be withheld. That is a decision for whoever is handling the request.

Requests that are manifestly unfounded

If we consider that a request is 'manifestly unfounded', we may refuse it. When a request is 'manifestly unfounded' is not defined in law. A request may be considered manifestly unfounded if it lacks credibility, displays fantastical elements, or is otherwise unrealistic.

For example, a request by an individual that the department provide the secret films they are making of him, or a request for alleged transcripts being made of the requestor's telephone calls.

A request may also be manifestly unfounded if it is clearly being made by an individual under a pseudonym e.g. for nuisance purposes.

Requests that are excessive

If a request is 'excessive' then we may refuse it. When a request is 'excessive' is not defined in law, but is illustrated by reference to requests that merely repeat the substance of similar requests.

Requests can also be considered for refusal on this basis if the requestor is asking for very substantial volumes of information, and it would arguably be disproportionate to respond to such an extensive request.

Information held on another's behalf, including private emails

Reasonable use of official email systems for personal business is permitted. Personal emails are considered to be held by the department on behalf of the individual, rather than held by the department in its own right.

Therefore any information in private emails is exempt from subject access requests, unless it concerns official business.

Parliamentary privilege

Personal data are exempt from subject access where exemption is required for avoiding an infringement of the privileges of either House of Parliament.

Crown honours, dignities and appointments

The right to subject access does not apply where personal data is processed for the purposes of:

(i) conferring by the Crown of any honour or dignity.

(ii) assessing someone's suitability for appointment to the following offices: (a) archbishops and diocesan and suffragan bishops in the Church of England; (b) deans of cathedrals of the Church of England; (c) deans and canons of the two Royal Peculiars;

(d) the First and Second Church Estates Commissioners; (e) lord-lieutenants; (f) Masters of Trinity College and Churchill College, Cambridge; (g) the Provost of Eton; (h) the Poet Laureate; (i) the Astronomer Royal.

Public appointments personal data in unstructured paper records

Where personal data is held in paper form outside of a 'filing system' (i.e. held outside a structured set of files where a person's data is readily accessible, such as customer or HR files), then it is exempt from the right of subject access if it concerns appointments, removals, pay, discipline, superannuation or other personnel matters in relation to: (a) service in the armed forces; (b) service in any office or employment under the Crown or under any public authority; (c) service in any office or employment, or under any contract for services, in respect of which power to take action, or to determine or approve the action taken, in such matters is vested in Her Majesty, ministers (including Welsh and Northern Irish government ministers), a public authority subject to the Freedom of Information Act 2000, or the Welsh Assembly.

Please note that in all other cases of personal data in unstructured paper records, the FoI cost limit applies (see FAQ).

Confidential references

Personal data is exempt from subject access if it consists of a reference given (or to be given) about the requestor in confidence for the purposes of education, employment, training, or an appointment.

Negotiations

Personal data that consists of a record of intentions in negotiations with an individual is exempt from the right of subject access to the extent that complying with the request would be likely to prejudice the negotiations.

Examination scripts

Personal data are exempt from subject access if they consist of information recorded by candidates during an exam.

Exam marks

This is not an exemption, but allows you to delay responding to a subject access request until after exam results have been published.

The deadline for responding to any subject access request for exam marks is extended until 40 days after those marks are published, or five months after receipt of the request.

Legal professional privilege

The right to subject access does not apply where the data consist of information in respect of which a claim to legal professional privilege could be maintained in legal proceedings.

Archiving in the public interest

The right of subject access does not apply where the personal data is processed for archiving purposes in the public interest to the extent that the application of those provisions would prevent or seriously impair the achievement of those purposes.

This is subject to the condition that the data is not used to make decisions about individuals, and the processing is not likely to cause substantial damage or distress.

Research and statistics

The right of subject access does not apply where the personal data is processed for (a) scientific or historical research purposes, or (b) statistical purposes, to the extent that the application of those provisions would prevent or seriously impair the achievement of the purposes in question.

This is subject to the condition that the data is not used to make decisions about individuals, the processing is not likely to cause substantial damage or distress, and the results of any resulting research does not identify individuals.

This exemption is principally to protect archives, libraries, etc from being subject to subject access requests in relation to their holdings.

National Security

The EU General Data Protection Regulation applies only to areas within the competence of the European Commission. That means that it does not apply to national security.

The Data Protection Act 2018 however extends nearly identical provisions to areas outside of EU competence, including national security. Section 26 of the DPA 2018 allows the right to make a subject access request to be disapplied where it is necessary to do so for the purpose of safeguarding national security.

Defence

The EU General Data Protection Regulation applies only to areas within the competence of the European Commission. That means that it does not apply to the Common Security and Defence Policy.

The Data Protection Act 2018 however extends nearly identical provisions to areas outside of EU competence, including defence. Section 26 of the DPA 2018 allows the right to make a subject access request to be disapplied where it is necessary to do so for defence purposes.

Other exemptions

Domestic use

Data protection legislation (including the right of subject access) does not apply to personal data processed for domestic, private purposes. This means that any personal information processed by private individuals is exempt. If information is however published to the world (e.g. on a website), then this falls outside the domestic use exemption.

Judicial appointments

The right to subject access does not apply where personal data is processed for the purpose of assessing someone's suitability for judicial office or Queen's Counsel.

Crime and taxation

The right to subject access does not apply where data is processed for, and release would be likely to prejudice, the purposes of:

- the prevention or detection of crime; or
- the apprehension or prosecution of offenders; or
- the assessment or collection of tax or duty or an imposition of a similar nature.

Personal data is also exempt if it is passed, by someone exercising the above functions, to another data controller for the purpose of discharging statutory functions.

Crime and taxation: risk assessment systems

Personal data is exempt from subject access where it consists of a classification applied to the data subject as part of a risk assessment system and responding to subject access would prevent that system from operating effectively. The risk assessment systems in question are those

(a) operated by a government department, a local authority or another authority administering housing benefit, and
(b) operated for the purposes of either the assessment or collection of a tax or duty or an imposition of a similar nature, or the prevention or detection of crime or apprehension or prosecution of offenders, where the offence concerned involves the unlawful use of public money or an unlawful claim for payment out of public money.

Immigration

The right to subject access does not apply where data is processed for the purpose of, and responding would prejudice, the following:

(a) the maintenance of effective immigration control, or
(b) the investigation or detection of activities that would undermine the maintenance of effective immigration control.

Personal data is also exempt if it is passed, by someone exercising the above functions, to another data controller who uses it for the purpose of the above functions.

Functions designed to protect the public (paragraph 7, part 2, Schedule 2)

The right of subject access does not apply where it would prejudice protective functions exercised for the purpose of preventing dishonesty, fraud, misconduct, mismanagement, maladministration or risk to health and safety.

See the legislation for further details.

Regulatory activity (paragraphs 8 and 9, part 2, schedule 2)

The right of subject access is disapplied where it would prejudice the functions of a regulator.

See the legislation for further details.

Self-incrimination

A person need not comply with any subject access request to the extent that it would, by revealing evidence of the commission of any offence, expose the person to proceedings for that offence.

This exemption does not apply where the offence is an offence under the Data Protection Act 2018, or perjury.

Corporate finance

Personal data are exempt from subject access if they relate to the providing of a corporate finance service, and responding would be likely to affect the price of any financial instrument, and either affect a person's decision to deal in or subscribe to an instrument, or have an effect on business activity, and have a prejudicial effect on the orderly functioning of markets.

Management forecasting or planning

Personal data that is processed for management forecasting and planning is exempt if releasing it would prejudice the business or other activity of the organisation. For example, if the organisation is planning a reorganisation and redundancy programme.

Journalistic, academic, artistic and literary purposes

Personal data is exempt from subject access if it is processed for the purposes of journalism, academic purposes, artistic purposes or literary purposes, and it is intended for publication in the public interest, and responding would be incompatible with those purposes.

Health, education and social work

Various exemptions from subject access are available to those who process social work or health data, or pupil records.

There are also exemptions for child abuse data, adoption, fertilisation and embryology information, statements of special educational needs, and parental order records and reports.

See schedules 3 and 4 of the Data Protection act 2018 for further details.