GRA

GIBRALTAR REGULATORY AUTHORITY

(15) The Right of Access

Guidance on the EU General Data Protection Regulation 2016/679 & Data Protection Act 2004

25th November 2020

IR03/19 v.2

CONTENTS

SUMMARY

- The EU General Data Protection Regulation 2016/679 ("GDPR") and the Data Protection Act 2004 ("DPA") give individuals (also known as 'data subjects') the right to require an organisation to allow them to find out what personal data the organisation hold about them, why they hold it and who they disclose it to. This right is commonly known as subject access.

- Data subjects are only entitled to their own personal data and subject access cannot be used to access information relating to other persons (unless the information is also about them or they are acting on the other person's behalf). On occasions, information may need to be redacted by the organisation.

- A subject access request ("SAR") does not have to specifically state it is a SAR or make reference to the legislation but must clearly convey that an individual is requesting their own personal data. It can be made to any part of an organisation, to any person or contact point within the organisation, and can be verbally or in writing (including by social media).

- Organisations should consider whether staff who regularly interact with individuals and conduct data processing activities may need specific training to identify and handle SARs. It is also good practice for an organisation to have a policy for recording SARs received, particularly those made by telephone or in person.

- Prior to complying with a SAR, an organisation must be satisfied that the person making the request is the individual that is the subject of the data being requested.

- Organisations must act on a SAR without undue delay and, subject to exemptions, at the latest within one month of receipt.

- Organisations must make genuine and extensive efforts to provide an individual submitting a valid SAR with their information for free, and, in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

- A request may be refused if one of the exemptions in the DPA applies. Also, if a SAR is "manifestly unfounded or excessive" the organisation may request a "reasonable fee" or may refuse to deal with it. Organisations should however note that they must establish, with supporting evidence, that on the specifics of the case, they are justified in their approach. The data subject must also be informed about the refusal, without undue delay and within one month of receipt of the SAR.

- It is a criminal offence, in certain circumstances and in relation to certain information, for a person to require another person to make a SAR.

- There are some distinctions with regards the handling of SARs by 'competent authorities' when the personal data is processed for law enforcement purposes.

- The Information Commissioner has various enforcement powers when dealing with failures to comply with a SAR and/or inadequate compliance with a SAR.

1. INTRODUCTION

In this Guidance Note, the Gibraltar Regulatory Authority as the Information Commissioner[1] provides guidance on Subject Access Requests[2] ("SARs").

Organisations need to be aware of an individual's right of access to their personal data under the EU General Data Protection Regulation 2016/679 (the "GDPR") and the Data Protection Act 2004 (the "DPA").

This document sets out key points that organisations need to be mindful of when handling SARs and provides practical tips to assist organisations to ensure that they are GDPR and DPA compliant when responding to SARs.

The Guidance Note also features an 8-point checklist of the foremost "Dos and Don'ts".

Acknowledgements

Where appropriate, Gibraltar's Information Commissioner will seek to ensure that locally published guidance notes are consistent with others made available by fellow Commissioners in other jurisdictions.

As well as reflecting the existing data protection standards and practices in Gibraltar, parts of this document reflect and/or incorporate the guidance from the UK's Information Commissioner's office.

[1] The Information Commissioner is the Chief Executive Officer of the Gibraltar Regulatory Authority.

[2] A request by an individual for his or her personal data under Article 15 of the GDPR is commonly referred to as a Subject Access Request.

2. WHAT IS THE RIGHT OF ACCESS?

In short, the right of access means that individuals have a right to obtain information that organisations hold about them. This is an important right, aimed at ensuring individuals have control over their information, and to enable them to be *"aware of and verify the lawfulness of processing*[3]*"*.

Data controllers are required, subject to limited circumstances (see section 7.9 on refusals), to provide data subjects with a copy of their personal data upon request.

In order to establish whether the information requested falls within the definition of 'personal data', it is important for data controllers to consider the broad definition of 'personal data'.

Personal data means **any information relating to an identified or identifiable natural person** ('data subject'); an identifiable natural person is one who can identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person[4].

The GDPR states that an individual's right to obtain a copy of their personal data must not adversely affect the rights and freedoms of others. An individual is therefore only entitled to their own personal data and the right cannot be used to access information relating to other persons (unless the information is also about them or they are acting on the other person's behalf).

In this respect, dealing with a SAR can be demanding and time-consuming, as sometimes, data will be unstructured and may relate not only to the data subject submitting the SAR, but also to other individuals. Nevertheless, a controller must still make genuine and extensive efforts to provide the individual submitting the SAR with their information (see section 7.7 on information of others).

There are some distinctions with regards the handling of SARs by 'competent authorities'[5] (see section 10) when it concerns personal data processed for law enforcement purposes, however, the regime is largely the same and the information in this Guidance Note should be useful for competent authorities too.

3. WHAT IS AN INDIVIDUAL ENTITLED TO?

Article 15 of the GDPR outlines the right of access and gives individuals the right to know, and have confirmed, whether a data controller is in fact processing their personal data. Should there be such processing, individuals are entitled to obtain the following from the data controller –

1) a copy of their personal data; and

[3] Recital 63 of the GDPR.

[4] Article 4(1) of the GDPR.

[5] Section 39 and Schedule 7 of the DPA.

2) other supplementary information as listed within Article 15 of the GDPR, which includes:

(a) The purpose(s) of the processing, in particular, if automated decision-making or profiling takes place, and if so, the logic involved, significance and likely consequences of such processing.

(b) The categories of personal data concerned.

(c) The recipients or categories of recipient the organisation discloses the personal data to.

(d) Retention periods for storing the personal data or, where this is not possible, the criteria for determining how long it will be stored.

(e) The existence of the individual's rights -

i. to request rectification of their personal data (see Article 16 of the GDPR - Right to rectification);
ii. to request the deletion or removal of personal data where there is no compelling reason for its continued processing (see Article 17 of the GDPR - Right to erasure);
iii. to block/suppress and ultimately restrict the processing of personal data (see Article 18 of the GDPR - Right to restrict processing);
iv. to object to such processing (see Article 21 of the GDPR - Right to object); and
v. to lodge a complaint with the supervisory authority i.e. the Information Commissioner.

(f) Information about the source of the data, where it was not obtained directly from the individual.

(g) The safeguards provided upon the transfer of personal data to a third country or international organisation.

Note: Competent Authorities processing personal data for law enforcement purposes should refer to **sub-sections 54(1) and 54(2) of the DPA** for a list of the information that they should provide when responding to a SAR.

If an organisation holds information about the requester otherwise than in electronic form (e.g. in paper files), they will need to decide whether it is covered by the right of subject access. The outcome will depend primarily on whether the non-electronic records are held in a 'relevant filing system' and also on whether the requester has given enough context to enable the organisation to find it. Broadly speaking, a relevant filing system exists where information about individuals is held in a sufficiently systematic, structured way, as to allow ready access to specific information about those individuals. Organisations must make every effort to locate the specific information and process the SAR accordingly.

4. HOW TO RECOGNISE A SAR

The GDPR does not specify how data subjects should make a valid request, which means an individual can make a SAR to any part of the organisation (including by social media). It does not have to be directed to a specific person or contact point, and it can be made verbally or in writing. It is important to recognise that verbal requests, which are not recorded, may be difficult to prove and follow up. It is therefore good practice to have a policy for recording details of the requests received, particularly those made by telephone or in person.

A request does not have to include the phrase 'subject access request', 'SAR', 'right of access' or make reference to 'Article 15 of the GDPR', but it must clearly convey that an individual is requesting their personal data.

The GDPR's right of access presents data controllers with the challenge of firstly establishing a request has been received, and then verifying whether it is a valid request.

Organisations may also wish to check with the requester to confirm that the content of the request has been properly understood, as this can help avoid later disputes about how the request has been interpreted.

In any event, data controllers have a legal responsibility to identify when an individual has made a SAR and it must be dealt with accordingly. In this regard, organisations may need to consider whether staff who regularly interact with individuals and engage in data processing activities may need specific training to identify and handle a SAR.

5. SHOULD ORGANISATIONS HAVE A SPECIALLY DESIGNED FORM FOR SARS?

Standard forms for SAR submissions may make it easier for the organisation to recognise the SAR and for the individual to include all the details required to locate the information they are requesting.

Recital 59 of the GDPR deals with procedures for the exercise of the rights of data subjects and recommends that organisations *'provide means for requests to be made electronically, especially where personal data are processed by electronic means*'. Organisations should therefore also consider designing a SAR form that individuals can complete and submit electronically.

However, even if a form is designed for SARs, organisations should note that a SAR is also valid if it is submitted by other means. Thus, organisations would still need to comply with all SAR requests whether received in letter form, by email or conveyed verbally, as submitting a SAR using a specially-designed form is not compulsory. Organisations should not use this as an excuse to extend the prescribed one-month time limit for responding.

6. HOW SHOULD THE PERSONAL DATA BE PROVIDED?

In brief, **Articles 12(5) and 15(3) of the GDPR** outline the following requirements for the provision of data:

1) Free first copy: Unless the controller can demonstrate the requests from the data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the first request for a copy of processed personal data shall be free. In the event a controller decides to charge a fee, they should contact the requester promptly to inform them of this. Any such fee should be *"a reasonable fee"* based on the costs of the administration involved in complying with the specific request.

2) Subsequent copies: Further requests for the same information may be charged "*a reasonable fee*" based on administrative costs.

3) Electronic copies: Where the request is made by electronic means, and unless otherwise requested by the data subject, electronic requests for data shall be provided in commonly used electronic form.

A best practice recommendation is that, where possible, organisations should be able to provide remote access to a secure self-service system which would provide the individual with direct access to his or her information[6]. Although this will not be appropriate for all organisations, there are some sectors where this may work well. Importantly, remote access should not adversely affect the rights and freedoms of others – including trade secrets or intellectual property.

6.1 An organisation receives a request but needs to amend the data before sending out the response. Should the "old" version be sent out?

It is the Information Commissioner's view that a SAR relates to the data held at the time the request was received. However, in many cases, routine use of the data may result in it being amended or even deleted while an organisation is dealing with the SAR. In such cases it would be reasonable for organisations to supply the information held at the point when the first response is sent out confirming receipt of the SAR, even if this is different to that held when the request was received.

It is **not** acceptable however to amend or delete the data if the organisation would not otherwise have done so. It is considered an offence, under data protection law, to make any amendment with the intention of preventing its disclosure (**sub-section 178(3) of the DPA**).

6.2 Are organisations expected to explain the contents of the information sent to the individual?

The GDPR requires that information be provided to an individual in a concise, transparent, intelligible and easily accessible form, using clear and plain language. This will be particularly important where the information is addressed to a child.

[6] Recital 63 of the GDPR.

This means that the additional information you provide in response to a request should be capable of being understood by the **average** person (or child). Organisations are not however required to ensure that that the information is provided in a form that can be understood by the particular individual making the request.

For further information about requests made by a child please refer to section 7.6.

Example A

An organisation receives a SAR and certain difficulties arise when preparing the response because a lot of the information requested is in coded form. For example, the information relating to the training sessions attended by the individual making the request are coded and logged as "P" on those the individual has participated in or logged as "M" for those missed. Further, some of the information is in the form of handwritten notes that are difficult to read.

Without direct access to the key or index used to explain the "P" and "M" coded information, it would be impossible for anyone outside the organisation to understand. In this case, the organisation would be required to explain the meaning of the coded information.

Additionally, whilst it may be good practice to decipher poorly written notes, the GDPR does not require organisations to make information legible, therefore organisations can simply provide a copy of the handwritten notes without further explanation.

Example B

An organisation receives a SAR from someone whose English comprehension skills are quite poor. A response is sent to the individual in line with GDPR requirements but that individual further requests that the organisation translate the information into simpler terms.

Organisations are not required to satisfy any further requests made by an individual in relation to the comprehension of the SAR's response if the response could be understood by the average person. Nonetheless, it would be good practice for the organisation to help individuals understand the information held about them.

7. PROCESSING A SAR

Processing SARs effectively and within the legal timeframe remains a challenge for many organisations especially where SARs are becoming increasingly onerous. For example, the amount of information held about employees and former employees (whether in a personnel file, internal memorandums, meeting notes or simply email correspondence) can be vast. Understanding from the outset how to respond to a SAR is crucial because failing to respond can expose the organisation to a claim, fines, enforcement action and/or reputational damage.

Organisations must act on the SAR without undue delay and at the latest **within one month of receipt**. The time limit should be calculated from the day the organisation receives the request (whether it is a working day or not) until the corresponding calendar date in the next month.

Example C

An organisation receives a request on the 1st September. The time limit will start from the same day. This gives the organisation until the 1st October to comply with the request.

Example D

An organisation receives a SAR on the 31sth March. The time limit will start from the same day. As there is no equivalent date in April, the organisation has until the 30th April to comply with the request.

If the 30th April falls on a weekend, or is a public holiday, the organisation has until the end of the next working day to comply.

Although the one-month time limit commences on the day of receipt of the SAR, there are instances during which time can be paused. For example:

1) If a controller validly requests a reasonable fee in order to process the SAR, time will pause when the controller requests this fee and will resume as soon as the fee is received.

2) If a controller requests clarity on the SAR, again the clock will stop at this point until a response from the data subject is received, at which point time will again continue to run.

3) If a controller requests further information to confirm the requester's identity, time will stop until the controller is reasonably satisfied as to their identity.

7.1 Can an organisation extend the time for a response?

The time to respond can be extended by a further two months beyond the initial one-month period if the request is complex or there have been a number of concurrent requests from the individual. The controller must however inform the individual of any extension within one month of receiving their request and explain why the extension is necessary.

7.2 Can an organisation ask an individual for ID?

A data controller must be satisfied that the person making the request is, in fact, the individual that is the subject of the data being requested. If there are doubts about the identity of the person making the request, organisations may ask for more information. It is important that only information that is necessary is requested to confirm an identity. The key to this is **proportionality**.

Organisations need to let the individual know **as soon as possible** that more information is required from them to confirm their identity before responding to their request. Again, note the pause in response-time as explained above.

It is important to note that there are often identification procedures already in place as data controllers regularly authenticate data subjects prior to entering into a contract or collecting his or her consent to the processing of their personal data. These procedures can form part of the identification measures used to handle SARs. As a consequence, when an individual has registered their details with an organisation, the personal data used to register the individual

concerned by the processing can also be used as evidence to identify them for SAR purposes. For example, where information and data collected online is linked to pseudonyms or unique identifiers (e.g. username and passwords), data controllers can implement appropriate procedures enabling an individual to make a SAR and receive the data relating to him or her. In essence, this would prevent an initial data controller from having to request additional information regarding a data subject's identity which could lead to excessive demands and the collection of personal data which are not relevant or necessary.

Example E

You have received a written SAR from a current employee. You know this employee personally and have even had a phone conversation with them about the request. Although your organisation's policy is to verify identity by asking for a copy of a utility bill, it would be unreasonable to do so in this case since you know the person making the request.

An organisation should not however always assume that the person making a request is who they say they are. In some cases, it is reasonable to verify their identity before sending any information to them.

Example F

An online retailer receives a SAR by email from a customer. The customer has not used the site for some time and although the email address matches the company's records, the postal address given by the customer does not. In this situation, before responding to the request it would be reasonable to gather further information, which could be as simple as asking the customer to confirm other account details such as a customer reference number.

How the SAR was made may also be of relevance when looking to confirm the requester's identity. For example, if the request is made via a social networking website, it would be prudent to check it is a genuine request.

In determining the proportionality of identity checks, organisations should take into consideration the possible harm and distress that inappropriate disclosure could cause to the individual to who the data belongs.

Example G

A GP practice receives a SAR from someone claiming to be a former patient. The name on the request matches a record held by the practice, but there is nothing else in the request to enable the practice to be confident that the requester is the patient to whom the record relates. In this situation, it would be reasonable for the practice to ask for more information before responding to the request. The potential risk to the former patient of sending their health records to the wrong person is such that the practice is right to be cautious.

7.3 What if a request is for large amounts of personal data?

If an organisation processes large amounts of information about an individual, more information may be required from the individual to clarify their request. Only information reasonably required to find the personal data covered by the SAR should be requested. However, if an individual refuses to provide any additional information, the organisation must still endeavour to comply

with the SAR (i.e. by making a reasonable effort to search/locate the information covered by the request).

This does not however mean that the controller needs to take disproportionate measures. For example, although there is a general obligation to supply a requester with information 'in permanent form', a controller is not required to do so if:

1) The requester agrees to another arrangement[7]; or

2) Where the supply of such a copy is impossible or would involve disproportionate effort[8].

'Disproportionate effort' is not defined in the DPA. The court[9] has however explained that organisations should assess, in the circumstances of a particular case, whether supplying a copy of the requested information in permanent form would result in so much work or expense as to outweigh the requester's fundamental right of access to their personal data. Organisations may take into account difficulties that arise throughout the process of complying with the request, including for example difficulty in locating the requested information (see 7.4 below).

Example H

An organisation has decided that to supply copies of an individual's records in permanent form would involve disproportionate effort. Rather than refuse the individual access, they speak to her and agree that it would be preferable if she visited their premises and viewed the original documents. They also agree that if there are documents she would like to take away with her, they can arrange to provide copies.

The burden of proof is on the data controller to show that they have taken all reasonable steps to comply with the SAR, and that it would be disproportionate in all the circumstances of the case for them to take further steps. Reasonable steps may for example include; engaging openly with the data requester in an attempt to reduce the costs and effort that the organisation would otherwise incur in searching for the requested information, or, making attempts to identify an alternative way of satisfying the request.

It is important to remember however, that even in the case that the information can't reasonably be provided in permanent form, the data subject still has the right to be provided with details of the personal data being processed, if any, as outlined at section 3.

7.4 What if we have difficulty in finding and/or retrieving the information?

The DPA places a high expectation on organisations to provide information in response to a SAR. It is important that information management systems are well-designed and maintained so that an organisation can efficiently locate and extract (or redact if necessary) personal data when required.

[7] Sub-section 104(1)(b) of the DPA.

[8] Sub-section 104(1)(a) of the DPA.

[9] Dawson-Damer & Ors v Taylor Wessing LLP [2017] EWCA Civ 74; Ittihadieh v 5-11 Cheyne Gardens RTM Co Ltd & Ors; Deer v University of Oxford and University of Oxford v Deer

Example I

A chain of hotels is dealing with a SAR from a member of staff. The person dealing with the request is satisfied that the staff member has been sent all information held in personnel files. However, the staff member complains that information was missing from the response.

The employer should not ignore this, but it would be reasonable to ask him for more details. For example, some of the information may be in emails, and the employer could reasonably ask for the approximate dates when the emails were sent and who sent them. He may also for example be seeking information that relates to a complaint he made as a customer and not as an employee and it would be reasonable for the employer to clarify this with the requester.

Importantly, an organisation cannot require the requester to narrow the scope of their SAR, so if a requester asks for 'all the information you hold' about them, they are entitled to do that. The organisation may however make attempts to ascertain details of the context and timeframe so as to more easily locate the data by for example asking if the data would be held electronically, if it relates to a particular timeframe etc.

In most cases, information stored in electronic form can easily be found and retrieved. However, information may have been archived or deleted and may therefore not be as readily accessible as on a 'live' system.

When information is archived it is often no longer required for general day to day business, although the organisation may envisage that a copy may be required in future. In such a case, there should be procedures to access this. As these procedures are often not as straightforward as for a 'live' system, the requester's ability to provide context may significantly affect whether the organisation can find what the requester wants. Nevertheless, to the extent that an organisation's search mechanisms allow them to find archived or backed-up data for their own purposes, they should use the same effort to find information in order to respond to a SAR.

If, however, a request relates specifically to back-up copies of 'live' data, and there is no evidence that there is any material difference between them, then there is no reason to provide the back-up data as well as the 'live' data.

With regards deleted data, organisations are not required to expend time and effort reconstituting information that they have deleted as part of their general records management if this would incur large fees or require substantial resources. The rationale is that, if the organisation has deleted the data it follows that they no longer require it and have no intention to process it further. Once deleted they can no longer use it to make decisions affecting the individual, therefore it can have no effect on the data subject. Nevertheless, if this data is fairly easily retrievable then they should also provide it.

For the avoidance of doubt, the contents of an email should not be regarded as deleted merely because it has been moved to a user's 'Deleted items' folder. It may be particularly difficult to find information to which a SAR relates if it is contained in emails that have been archived and removed from an organisation's 'live' systems. Nevertheless, the right of subject access is not limited to the personal data which it would be easy to provide. The organisation may, of course, ask the requester to give them some context that would help to find what they want.

7.5 What about requests made on behalf of others?

The GDPR does not prevent an individual from making a SAR via a third party. Often, this will be a solicitor acting on behalf of a client, but it could simply be that an individual feels comfortable allowing someone else to act on their behalf. In these cases, an organisation will need to be satisfied that the third party making the request is entitled to act on behalf of the individual, but it is the third party's responsibility to provide evidence of this entitlement. This might be a written authority to make the request or it might be a more general power of attorney.

Should an organisation believe an individual may not understand what information would be disclosed to a third party who has submitted a SAR on their behalf, they may send the response directly to the data subject rather than to the third party. The data subject may then choose to share the information with the third party after having had a chance to review it.

7.6 What if the request is for information about children?

Even if a child is too young to understand the implications of the right of access, it is still the right of the child rather than of anyone else such as a parent or guardian. It is therefore the child who has a right of access to the information held about them, even though in the case of young children these rights are likely to be exercised by those with parental responsibility for them.

Before responding to a SAR concerning information held about a child, data controllers should consider whether the child is mature enough to understand their rights. If the controller is confident that the child can understand their rights, then they should usually respond directly to the child. A controller may, however, allow the parent to exercise the child's rights on their behalf if the child authorises this, or if it is evident that this is in the best interests of the child.

What matters is that the child is able to understand (in broad terms) what it means to make a SAR and how to interpret the information they receive as a result of doing so.

When considering borderline cases, it is important that organisations take the following into account, amongst other things:

1) the child's level of maturity and their ability to make decisions like this;

2) the nature of the personal data;

3) any court orders relating to parental access or responsibility that may apply;

4) any duty of confidence owed to the child or young person;

5) any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment;

6) any detriment to the child or young person if individuals with parental responsibility cannot access this information; and

7) any views the child or young person has on whether their parents should have access to information about them.

7.7 What should we do if the data includes information about other people?

Responding to a SAR may involve providing information that relates both to the individual making the request and to another individual.

In this respect, **sub-section 18(2) of the DPA** states that –

> *"nothing […] obliges a data controller to disclose personal data relating to an individual other than the individual making the request unless that individual has consented to the disclosure or cannot be identified from the data, save where the circumstances are such that it would be reasonable for the data controller to conclude that, if any particular identifying the other individual were omitted, the data could then be disclosed without his being thereby identified to the data subject, the data controller shall be obliged to disclose the data to the data subject with the omission of those particulars".*

Therefore, although controllers may sometimes be able to disclose information relating to a third party, they need to decide whether it is appropriate to do so in each case. This will involve balancing the data subject's right of access against the other individual's rights and may also include, for example, contacting the other individual to enquire whether they would consent to the disclosure of their personal data in response to the SAR. If the other person consents to you disclosing the information about them, then it would be unreasonable not to do so. However, if there is no such consent, it is up to the data controller to decide whether to disclose the information anyway.

In determining whether it is reasonable to disclose the information, an organisation "*must not apply a blanket policy of withholding [the identities of other individuals]"* in responding to a SAR but must instead, make a *"detailed assessment of this issue"*[10]*.* They should take into account all of the relevant circumstances, including:

1) the type of information that would be disclosed;

2) any duty of confidentiality owed to the other individual;

3) any steps taken to seek consent from the other individual;

4) whether the other individual is capable of giving consent; and

5) any express refusal of consent by the other individual.

Additionally, they should consider whether the information is able to be redacted so as to remove any references that may identify the third party. Redaction may include for example 'blanking out' certain parts of a document or using technological means to 'blur' faces on CCTV footage. Crucially, redaction not only includes removing forms of direct identification (e.g. name, address etc.), but also information which may lead to an individual being identified (e.g. job title, vehicle registration plates etc.).

For the avoidance of doubt, controllers cannot refuse to provide access to personal data about an individual simply because they obtained that data from a third party. The rules about third party data apply only to personal data which includes both information about the individual who

[10] *Rudd v Bridle & Anor [2019] EWHC 893 (QB)*

is the subject of the request and information about someone else. In such cases the court[11] has observed that:

1) Data controllers should be afforded a wide margin of appreciation when reaching evaluative judgments between privacy rights and other interests;

2) There is no obvious priority between the interests of a requester and an objector;

3) The fact that the requester might be seeking the information with a view to litigation should not interfere with the data controller's assessment;

4) A data controller might consider whether to disclose information on the condition that an assurance or binding contractual undertaking is made that the information will not be disseminated more widely.

7.8 If we use a processor, does this mean they would have to deal with any SAR we receive?

Responsibility for complying with a SAR lies with the data controller. Data controllers need to ensure that they have contractual arrangements in place to guarantee that SARs are dealt with properly, irrespective of whether they are sent directly to the controller or to the processor.

Data controllers must not extend the one-month time limit on the basis that they have to rely on a processor to provide the information needed to respond. As mentioned above however, if the request is complex or a controller has received a number of requests from the individual, the time limit may be extended by a further two months, although there is still an obligation to contact the data subject within the first month.

7.9 Can we refuse to comply with a SAR?

A request may be refused if one of the exemptions as set out in the DPA applies (see section 8). Organisations should however be mindful when wishing to rely upon an exemption of the fact that they must establish, with supporting evidence, that the requirements of the relevant exemption are met on the specifics of the case. Failure to do so will likely result in a finding that the relevant exemption is not applicable, forcing the organisation to disclose the requested personal data.

Additionally, if an organisation considers that a request is *"manifestly unfounded or excessive"* they may request a *"reasonable fee"* to deal with the request or may refuse to deal with the request (see section 9).

7.10 What should we do if we refuse to comply with a request?

It is imperative that the individual is informed about the refusal to comply with the request without undue delay and within one month of receipt of the request. The individual should be advised about the following:

1) the reasons the controller is not taking action;

[11] This point was considered by the Court of Appeal in *B v General Medical Council [2018] EWCA Civ 1497* (Note although the case was heard under the previous UK legislation and not the current legislation, the principles continue to apply, also applying to the DPA 2004). The case considered the balancing exercise that needs to be carried out when a SAR is made and a third-party objects to their data being disclosed. In that case, a doctor objected to the production of his report when a patient sought and obtained it from the General Medical Council through a SAR. The Court of Appeal held that, on the facts of the case, the council was entitled to provide the data subject with the report.

2) their right to make a complaint to the Information Commissioner or other relevant supervisory authority; and

3) their ability to seek to enforce this right through a judicial remedy.

As foregoing, the organisation should also document the decision.

7.11 Can I require an individual to make a subject access request?

Under **sub-sections 18(5) and 18(6) of the DPA**, **it is a criminal offence**, in certain circumstances and in relation to certain information to require another person (or a third party) to submit a SAR. This is because of the importance of subject access as a core data protection right, as well as due to the fact that a SAR may disclose personal information which is excessive to the purposes. The provisions read as follows:

> *"18(5) A person shall not, in connection with*
> *(a) the recruitment of another person as an employer;*
> *(b) the continued employment of another person; or*
> *(c) a contract for the provision of services to him by another person,*
> *require that other person to make a subject access request or to supply him with data relating to that other person obtained as a result of such a request.*
>
> *18(6) A person who contravenes subsection (5) shall be guilty of an offence."*

The use of the words 'in connection with' mean that this subsection has a broad scope.

Example J

An individual applies for a position as a receptionist but is told that they cannot be offered the position until they provide a copy of their criminal record. The employer tells them they must submit a SAR to the Royal Gibraltar Police in order to gain this information and they will only be appointed if it is supplied.

The employer is likely to have committed an offence under section 18 of the DPA.

8. EXEMPTIONS

The DPA recognises that in some circumstances an organisation might have a legitimate reason for not complying with a SAR. It therefore provides a number of exemptions from the duty to comply. **The exemptions are mostly detailed in schedules 2 - 4 of the DPA**.

Organisations must however be prepared and able to defend their decision when relying on an exemption. It is therefore good practice to ensure that such a decision is taken at a suitably senior level and that the reasons for it are documented.

Whether an exemption applies will be dependent on the facts. Again, depending on the circumstances, the organisation may refuse to provide all or some of the information requested. It is an organisation's choice whether they wish to rely on an exemption or not, as, even though an exemption may apply, they may still decide to provide the information requested.

Notably, exemptions may apply for different reasons. Some apply because of the nature of the personal data in question (e.g. information contained in a confidential reference), whereas others may apply because disclosure of the information would be likely to prejudice a particular function of the organisation to which the request is made. Importantly, the DPA does not explain what is meant by 'likely to prejudice', although the Information Commissioner's view is that it requires there to be a substantial chance that complying with the SAR would noticeably damage the discharge of the relevant function.

By way of example, we provide below some situations in which organisations may be unclear as to whether they need to comply or not. Importantly, the facts of each case should be looked at in themselves and what may apply to one organisation or piece of data may not apply to another. Additionally, this is not intended to be an exhaustive list and there are other applicable circumstances.

1) Confidential references[12]

   This exemption applies if you give or receive a confidential reference for the purposes of prospective or actual:

   (a) education, training or employment of an individual;

   (b) placement of an individual as a volunteer;

   (c) appointment of an individual to office; or

   (d) provision by an individual of any service.

2) Crime and Taxation[13]

   Personal data processed for certain purposes related to crime and taxation is exempt from the right of subject access. These purposes include:

   (a) the prevention or detection of crime;

   (b) the capture or prosecution of offenders; and

   (c) the assessment or collection of tax or duty.

   However, the exemption applies only to the extent that complying with a SAR would be likely to prejudice the crime and taxation purposes to which particular personal data relates, and it may be that some of the data is disclosable while other parts are subject to the exemption.

   Personal data that:

   (a) is processed for the purpose of discharging statutory functions; and

   (b) consists of information obtained for this purpose from someone who held it for any of the crime and taxation purposes described above is also exempt from the right of

[12] See Schedule 2, part 4, paragraph 19 of the DPA
[13] See Schedule 2, part 1, paragraph 2 of the DPA

subject access to the extent that providing subject access to the personal data would be likely to prejudice any of the crime and taxation purposes.

This prevents the exemption from being lost when personal data is disclosed by law-enforcement agencies to an organisation that requires it for the performance of a statutory function.

3) Regulatory activity[14]

Some organisations may use an exemption from subject access if they perform regulatory activities. This only applies to organisations that have regulatory functions concerning the protection of the public or charities, or fair competition in business. Again, organisations that do have such functions may only apply the exemption to personal data processed for these core regulatory activities, and then only to the extent that granting subject access to the information concerned would be likely to prejudice the proper discharge of those functions.

4) Legal advice and proceedings[15]

Personal data is exempt from the right of subject access if it consists of information for which legal professional privilege could be claimed in legal proceedings. This encompasses privileged information relating to both 'legal advice' and 'litigation'. Information that comprises confidential communications between client and professional legal adviser may be withheld under the legal privilege.

Where legal professional privilege cannot be claimed, the organisation may not refuse to supply information in response to a SAR simply because the information is requested in connection with actual or potential legal proceedings. Additionally, there is nothing in the DPA that limits the purposes for which a SAR may be made, or which requires the requester to tell the organisation what they want the information for.

9. MANIFESTLY UNFOUNDED OR EXCESSIVE REQUESTS

If you process personal data, you may refuse to respond to certain SARs if you can demonstrate that they are **manifestly unfounded** or **excessive.**[16]

Alternatively, you may choose to respond to a SAR that may be regarded as manifestly unfounded or excessive and charge a reasonable fee for doing so.[17]

[14] See Schedule 2, part 2, paragraph 6 of the DPA

[15] See Schedule 2, part 4, paragraph 14 of the DPA

[16] See Article 12(5)(b) of the GDPR. For law enforcement related processing by a competent authority please see Part III, Chapter 3, Section 62(1)(b) of the DPA.

[17] See Article 12(5)(a) of the GDPR. For law enforcement related processing by a competent authority please see Part III, Chapter 3, Section 62(1)(a) of the DPA.

Organisations should steer clear from establishing a blanket policy for determining whether a SAR is manifestly unfounded or excessive. Each SAR must be considered on a case-by-case basis. Whilst there may be characteristics that are indicative of a manifestly unfounded or excessive request, organisations should only use these as a guide and not automatically presume that the submission of a SAR is manifestly unfounded or excessive just because the individual has previously submitted requests, or if such previous requests have been duly classified as being manifestly unfounded or excessive.

9.1 What does manifestly unfounded mean?

A SAR may be **manifestly unfounded** if the individual has no clear intention to access the information, or if the individual is malicious in their intent, using such request to harass an organisation with no real purposes other than to cause disruption.

Example K

An individual submits a SAR to an online retail company and reiterates that he is making a SAR in accordance with data protection law. In his communication, the individual states that if the company credits his account with a specified sum of money, he will withdraw the SAR. The organisation in question would be correct to consider this SAR to be manifestly unfounded.

The following factors, amongst other things, may indicate malicious intent –

1) the individual has explicitly stated, in the request itself or in other communications, that they intend to cause disruption;

2) the request makes unsubstantiated accusations against you or specific employees;

3) the individual is targeting a particular employee against whom they have some personal grudge; or

4) the individual systematically or frequently sends different requests to the organisation as part of a campaign with the intention of causing disruption.

The above-mentioned factors are not intended as a check-list that automatically means a SAR is manifestly unfounded. It is important that the organisation consider all SARs in the context in which they are made, and the **onus** is on the organisation to **demonstrate** that the SAR is manifestly unfounded.

It should be noted that the inclusion of the word "manifestly" means it must be obvious and clear that the SAR is unfounded. It is unlikely that an individual who genuinely wants to exercise his/her rights presents an organisation with this situation. Further, in most cases, the use of aggressive or abusive language does not, in itself, demonstrate a request to be manifestly unfounded.

Example L

An individual believes that information held about them is inaccurate. The individual repeatedly requests its correction but the organisation advises that they regard the information to be accurate and demonstrates that the matter has been previously investigated. The individual continues to submit further SARs along with unsubstantiated claims against the organisation.

The organisation refuses the most recent SAR because it is manifestly unfounded, and the individual is notified of same.

9.2 What does excessive mean?

Whether a SAR is excessive, or manifestly excessive, depends on the particular circumstances. An organisation should primarily consider whether the SAR is clearly or obviously unreasonable, basing this on whether the SAR is proportionate when balanced against the burden or costs involved in processing said request.

A request may be **excessive** if for example:

1) it repeats the substance of previous requests and a reasonable interval has not elapsed; or

2) it overlaps with other requests for the same information.

Again however, the specific facts must be considered. A SAR will not necessarily be excessive just because the individual requests a large amount of information, even if providing this might be burdensome. Instead of refusing, the organisation can attempt to clarify the request to specifically locate what the individual wants. Similarly, if a data subject requests further copies of their information, this is unlikely to be a ground for refusal. A controller can however charge a reasonable fee for the administrative costs of providing this information again.

Example M

A library receives a SAR from an individual who made a similar request one month earlier. The information relates to when the individual joined the library and the items borrowed. None of the information has changed since the previous request. With this in mind, along with the fact that the individual is unlikely to suffer any disadvantage if the library does not send any personal data in response, the library need not comply with this request. However, it would be good practice to respond explaining why the information has not been provided again.

Importantly, the GDPR and DPA do not limit the number of SARs an individual can make to the same organisation. Requests about the same issue are not always excessive. An individual may have legitimate reasons for making requests that repeat the content of previous requests. For example, if the organisation has not handled previous requests properly. In such cases where an individual may wish to receive another copy of the information they had previously requested, the organisation may charge a reasonable fee for the administrative costs of providing the information again. It is unlikely that this is an excessive request.

Example N

A therapist who offers non-medical counselling receives a SAR from a client. She had responded to a similar request from the same client three weeks earlier. When considering whether the requests have been made at unreasonable intervals, the therapist should take into account the fact that the client has attended five sessions between requests, so there is a lot of new information on file. She should respond to this request, but could also ask the client to agree that she only needs to send any 'new' information. It would also be good practice to discuss with the client a different way of allowing the client access to the notes about their sessions.

Organisations should allow for some discretion when dealing with requests that are made at unreasonable intervals. When deciding whether a **reasonable interval** has elapsed, organisations should consider:

1) the nature of the data (e.g. whether particularly sensitive);

2) the purposes of the processing (e.g. if disclosure is likely to be detrimental to the requester); and

3) how often the data is altered (e.g. if information is likely to have changed between requests).

Although organisations are not obliged to comply with identical or similar requests they have already dealt with unless a reasonable interval has elapsed between the requests, if information has been added to or amended since the earlier request, the organisation is required to provide a full response to the request, not merely an update to the previous request. In practice however, organisations can attempt to negotiate with the requester to restrict the scope of the SAR to the new or updated information. If however the data subject insists upon a full response, then the organisation must supply all the information.

Importantly, if an organisation deems that the SAR is manifestly unfounded or excessive, the organisation must be able to demonstrate this to the individual and/or to the Information Commissioner.

10. SARS TO 'COMPETENT AUTHORITIES'

Processing by *"competent authorities"*[18] for *"law enforcement purposes"*[19] falls outside the scope of the GDPR. This type of processing is however covered by Part 3 of the DPA, which ensures a subject's personal data rights with regards competent authorities are of similar standards to those under the GDPR.

Section 54 of the DPA governs the right of access by a data subject with respect to personal information processed by competent authorities. A data subject is generally entitled to the same data as they would be if they were submitting the SAR to any other controller[20]. However, with respect to competent authorities, **sub-section 54(4) of the DPA** provides that:

> *"The controller may restrict, wholly or partly, the rights conferred by subsection (1) to the extent that and for so long as the restriction is, having regard to the fundamental rights and legitimate interests of the data subject, a necessary and proportionate measure to-*
> *(a) avoid obstructing an official or legal inquiry, investigation or procedure;*
> *(b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;*
> *(c) protect public security;*
> *(d) protect the security of Gibraltar;*
> *(e) protect the rights and freedoms of others".*

[18] Refer to Section 39 of the DPA for definition.

[19] Refer to Section 40 of the DPA for definition.

[20] Refer to Sub-section 54(1) and 54(2) of the DPA.

Any decision to apply this sub-section must be recorded and the decision conveyed to the data subject in writing and without undue delay including, in accordance with **sub-section 54(5) of the DPA**:

> *"(5) Where the rights of a data subject under subsection (1) are restricted, wholly or partly, the controller must inform the data subject in writing without undue delay-*
>
> *(a) that the rights of the data subject have been restricted;*
> *(b) of the reasons for the restriction;*
> *(c) of the data subject's right to make a request to the Commissioner under section 60;*
> *(d) of the data subject's right to lodge a complaint with the Commissioner; and*
> *(e) of the data subject's right to apply to a court under section 172".*

There is however an exemption to **subsections 54(5)(a) and 54(5)(b) of the DPA** in that they do not apply to the extent that the provision of the information would undermine the purpose of the restriction[21].

Example O

A law enforcement body receives a SAR from an individual who is under investigation but is not aware of this. The details of the investigation comprise all the information held about the data subject.

In such a case, informing the data subject that their rights have been restricted under **sub-section 54(4)(b) of the DPA** could potentially alert the data subject to the existence of the investigation and could lead to the investigation being compromised.

In addition to the above, **sub-section 52(3) of the DPA** provides that the subject access rights do not apply in relation to the processing of *"relevant personal data"* i.e. personal data contained in a judicial decision or in other documents relating to the investigation or proceedings which are created by or on behalf of a court or other judicial authority. In such circumstances, access to such data will instead be governed by the appropriate legislation covering the disclosure of information in criminal proceedings e.g. the Criminal Procedure and Evidence Act 2011.

Importantly, **sub-section 52(3) of the DPA** only applies where the judge or other judicial authority is the controller and the relevant personal data is contained in a judicial decision or in other documents which are created during a criminal investigation or proceedings and made by or on behalf of the judge or judicial authority. So, for example, where a competent authority is commissioned by a court or other judicial authority to create a document, the provisions in **sub-section 52(3) of the DPA** extend to that document and the personal data contained within it. The original personal data processed by the competent authority used to inform the document will however remain subject to the provisions of the DPA.

[21] See sub-section 54(6) of the DPA

11. INADEQUATE OR NON-COMPLIANCE WITH A SAR

Under Part VI of the DPA, the Information Commissioner has various enforcement powers when dealing with the failure by an organisation to comply with relevant data protection legislation, including failure to comply with a SAR (this may include not responding and/or responding inadequately to a SAR).

Within these powers the Information Commissioner can:

1) Issue Information Notices;

2) Issue Assessment Notices;

3) Issue Enforcement Notices;

4) Enter and Inspect (upon obtaining a warrant from the courts);

5) Issue a reprimand to the relevant organisation; and/or

6) Impose a monetary penalty on the organisation.

When considering the appropriate sanction(s) to impose, the Information Commissioner is under an obligation to consider taking action that is both proportionate and effective.

In addition, **sub-section 172(1) of the DPA** gives a data subject the right to apply to court if they feel there has been a breach of their rights under data protection law, including an infringement of their right to access their personal data.

Under **sub-section 172(2) of the DPA**, the court may make an order "for the purposes of securing compliance". The court must however first verify that there has been a breach, and, if it decides there has in fact been a breach, when exercising its discretion it must ensure to take proportionate action and must seek a fair balance between the rights of the data subject and the interests of the data controller[22].

12. "DOS AND DON'TS" CHECKLIST

The checklist overleaf provides a summary of the foremost "dos and don'ts" that organisations should take into account when processing a SAR.

[22] As noted in *Lindqvist (Case C-101/01) [2004] All ER (EC) 561, paragraph 90*

DOS AND DON'TS

1. **DO NOT IGNORE** a SAR because this can lead to financial penalties, enforcement action, legal proceedings and/or reputational damage.

2. **DO NOT DELAY**. Dealing with a SAR is time-consuming but time limits apply, so engage the appropriate personnel and start processing the request upon receipt.

3. Liaise with the individual if you need further information to **VERIFY THEIR IDENTITY** or to enable you to locate the requested information. Organisations must not shy away from cooperating with and/or engaging with the individual making the request.

4. **LOCATE** the personal data. Consider searching electronic systems and manual filing systems, back up data and any third-party data processors (e.g. payroll services) who may also hold relevant personal data.

5. **REDACT** information relating to other individuals unless (a) you have their consent, or (b) it is reasonable in all the circumstances to provide that specific information.

6. Consider whether an **EXEMPTION** applies, and also whether the request is **MANIFESTLY UNFOUNDED OR EXCESSIVE.**

7. **RESPOND** to the request within the one-month timeframe, providing copies of the relevant data and explaining, if and why, you are relying on any of the exemptions.

8. In the event that you refuse to comply with a request, **ADVISE** and **INFORM** the individual accordingly.

IMPORTANT NOTE

This document updated guidance previously published by the Information Commissioner on the subject matter. The document is purely for guidance purposes and does not constitute legal advice or legal analysis. All organisations that process personal data need to be aware that the GDPR and the DPA will apply directly to them. The responsibility to become familiar with the GDPR and the DPA and comply with its provisions lies with the organisation.

Where necessary, the Information Commissioner will review this Guidance Note in accordance with any updates or other developments. In the event of any conflict or inconsistencies between this Guidance Note and the GDPR and the DPA, the GDPR and the DPA will take precedence.

CONTACT US

Gibraltar Regulatory Authority
2nd floor, Eurotowers 4, 1 Europort Road, Gibraltar

(+350) 20074636
privacy@gra.gi
www.gra.gi