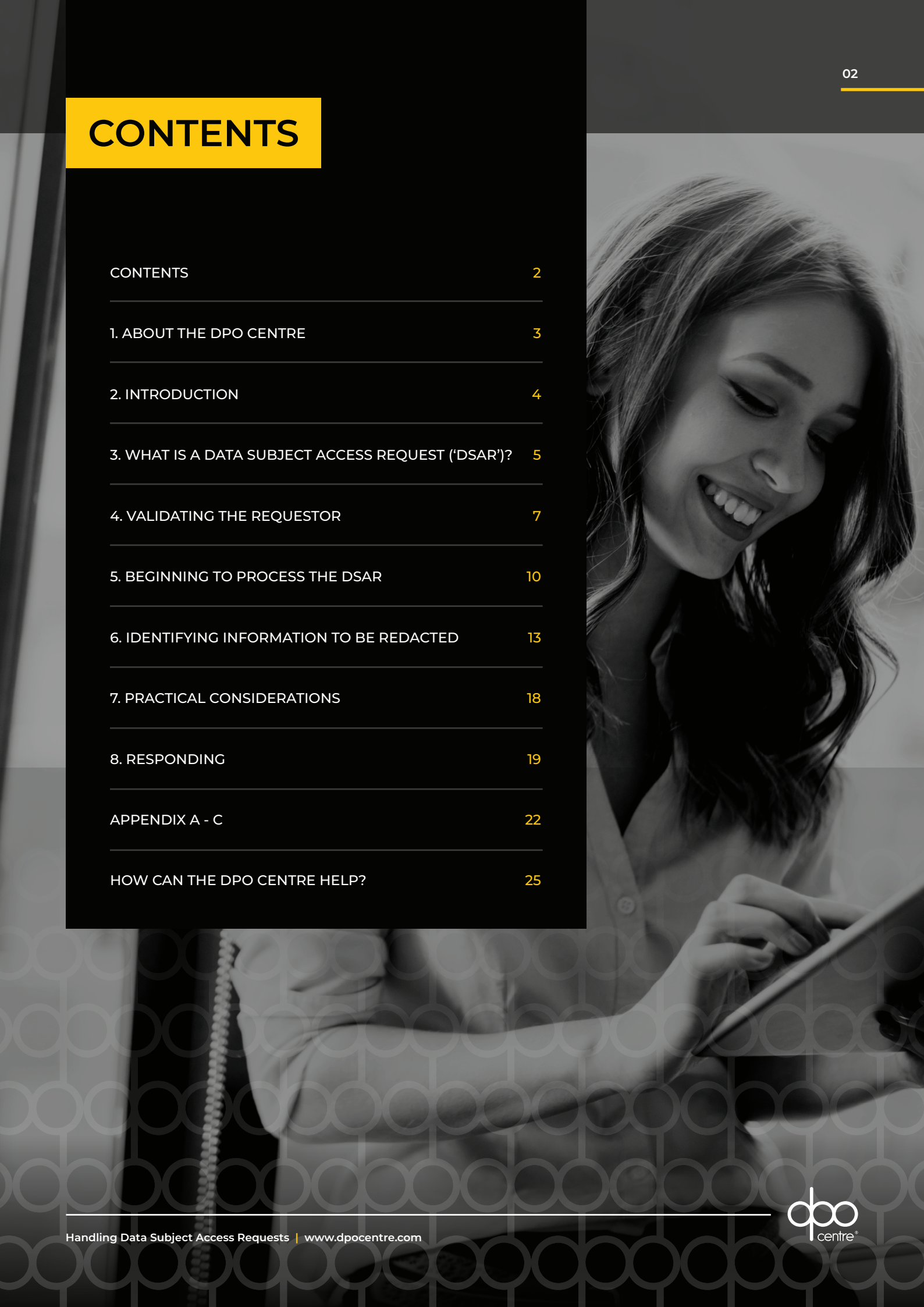
HANDLING DATA SUBJECT ACCESS REQUESTS *(DSARs)*

www.dpocentre.com

dpo centre®

CONTENTS



1. ABOUT THE DPO CENTRE

The DPO Centre is a specialist data protection and compliance consultancy, providing data protection related services to over 1,000 clients from a wide variety of sectors, ranging from commercial, financial services, tech, health, education and 3rd sector organisations.

Formed in July 2017, The DPO Centre delivers consultancy, gap analysis, staff training and a DSAR response service, alongside our core business of providing outsourced Data Protection Officers (DPOs). These services are provided on a 'fractional' basis, so range from one to eight days per month, dependent on the appropriate level of need.

Further information about our DSAR response service can be found on page 24, and details on the company, staff and our services can be found on our website.

2. INTRODUCTION

The implementation of the General Data Protection Regulation ('GDPR') and the Data Protection Act 2018 has seen a significant number of individuals ('Data Subjects') invoking their rights permitted by law. Whilst data protection law and other statutory provisions may give access to information (such as the Freedom of Information Act 2000), it is important that such requests are handled fairly, ensuring that the application of these rights do not undermine other obligations on you (such as preserving the data protection or privacy rights of other third parties, preserving any confidential duties, ensuring the non-prejudicing law enforcement activity etc.).

This guide aims to walk you through the journey of completing a Data Subject Access Request ('DSAR'). Whilst it is not exhaustive and is not specifically tailored to your company or your sector, it is indicative of some of the general considerations you will be expected to address when dealing with DSARs.

DSARs can be complex by their nature. It is not uncommon for professionals, including data protection professionals, to have a variety of different views on how to approach DSARs (such as when redactions should apply). If you remain unsure, it is important that you seek further advice or guidance from your Data Protection Officer (DPO) or from a specialist.

Please note that this guide does not aim to change your usual working practices. For example, if a bank routinely provides copies of statements on a monthly basis, it would not necessarily consider a request for an up-to-date bank statement from a verified customer as a DSAR. This guide will cover those instances which are out of the ordinary, which specifically mention data protection or subject access, or are seeking access to a large volume of records.

3. WHAT IS A DATA SUBJECT ACCESS REQUEST ('DSAR')?

Data subjects have a right to know that your company is processing their personal data, a copy of such personal data and other supplementary information regarding the nature and scope of their processing. The latter of which should form part of your Privacy Policies/Notices. Such requests mainly manifest themselves in data subjects seeking access to their own personal data, as part of a DSAR. However, the provision of copies of their personal data can often deliver several challenges and questions, such as:

- What happens if records containing their personal data also contain personal data of a third party?
- What happens if their personal data was provided to you in confidence, such as from a confidential informant?
- What happens if their request is time consuming or particularly voluminous?
- What happens if someone is requesting it on behalf of them?

These, amongst others, are considerations which you will need to address as part of responding to a DSAR and this guide aims to support you through this.

3.1 RECOGNISING A DSAR

There is no set form in which a DSAR may arrive. Data subjects can make their requests verbally or in writing. Whilst you may advise data subjects to complete a form or use a template from your website, there is no obligation on them to do so. Requests more often than not, will come in similar mould to that of the **template guidance issued by the Information Commissioner's Office**. The request need not mention the provisions of the GDPR, the Data Protection Act 2018 or the provisions of DSARs, it is your responsibility to identify and interpret it accordingly. However, usually these phrases will be utilised allowing for easy identification.

The important thing to remember is that commonly, a DSAR will be an individual (or someone acting on their behalf), seeking access to their own personal data or seeking clarity on how their personal data is being processed. If the request is seeking access to information other that the data subject's personal data (i.e. belonging to a 3rd party) then this should be refused.

You may also often find data subjects citing the Freedom of Information Act 2000 in an attempt to seek access to their own personal data. It should be noted that the Freedom of Information Act 2000 only applies in respect of public authorities (e.g. local councils, schools and hospitals), so unless you are a public authority, the obligation to respond to such requests does not apply. However, if it is clear that the request is a DSAR, then there is an obligation on you to treat it accordingly.

3. WHAT IS A DATA SUBJECT ACCESS REQUEST ('DSAR')? CONT...

3.2 WHAT SHOULD I DO IF I RECEIVE ONE?

It is important that you know your company's approach to dealing with such requests. This might be found in your Data Protection Policy. If no such process or document exists, then potentially it would be useful to define one at this stage. It is particularly important to clarify who within your company will be dealing with the request and who to forward them too.

3.3 TIME FRAMES TO RESPOND

You have a one calendar month time frame to respond to DSARs, with the clock starting on the day that the request is received, except where:

- the data subject has not provided enough information for you to identify the data they are requesting. Go back to them and ask them to clarify their request (the one-month will only start running on the day they supply you with the additional details you need to process the request); or
- the request is complex or the individual has made a number of requests (if you feel unable to deal with the matter in the next month, then your company can extend the timescale for responding on a month-by-month basis up to a maximum of two months)

Whatever decision is reached, it is vitally important to document it along with the reasoning. This demonstrates that you have considered the DSAR appropriately and not immediately jumped into relying on the two-month extension. If the extension is used, it must be communicated to the subject within the one-month period following the request and as soon as possible upon making the decision. The company cannot wait until the last day to use the extension. Once the decision has been made to extend, it must be communicated to the subject. From that point, the company will have two months regardless of how many of the original one month was left.

In this context 'complex' means the complexity of the request made by the data subject, not how difficult it would be for the organisation to access and supply the information. The Data Protection Act 2018 does not provide any guidelines as to what might qualify as a complex request, it will be for the company to make a judgement call taking into account all the facts of the case.

If the response date falls on a weekend or a public holiday, you have until the next working day to respond. This means that the exact number of days you have to comply with a request varies, depending on the month in which the request was made. If a consistent number of days is required (e.g. for operational or system purposes), you should consider adopting a 28-day period to ensure compliance is always within a calendar month.

4. VALIDATING THE REQUESTOR

It is crucial to validate who the requestor is. Depending upon who they are will dictate what rights are available to them and how their request should be processed. As indicated previously, the right of access is a personal right and in theory should only be initiated by the data subject themselves, but it should be noted that they also could delegate this right to someone working on their behalf (such as a trade union representative, their solicitor, a partner etc.). You will also get occasions whereby third parties will attempt to obtain information about others, sometimes these may be lawful and permissible by law (such as supporting the police with an investigation) but there will be occasions where people without lawful excuse will attempt social engineering, impersonation or 'blag' to access information.

4.1 PRACTICAL CONSIDERATIONS

If the request appears to come from the data subject it is still prudent to check who they are, as:

- Anyone can create an email address impersonating someone else
- A spouse or a third party could have access to their email account on a shared device
- Email addresses can be spoofed
- Someone can pretend to be working on behalf of them
- Blaggers and private investigators are known to have used such methods

The identity of individuals can be validated in a number of ways:

- Asking them to provide their request in writing along with copies of official identification documents, such as a passport, bank statement, utility bill, council tax bill, driving licence, medical card etc
- Establishing that it is a regular email address that they use to correspond with you and it is not newly made up
- Phoning them up on the telephone numbers you have recorded against them in your database, not the one they provide
- Asking security questions to which only they would know the answer

4. VALIDATING THE REQUESTOR CONT...

4.2 ARE THEY A 3RD PARTY ACTING ON THE DATA SUBJECT'S BEHALF?

An individual can delegate their rights to access their personal data to someone who is working on their behalf. However, in such instances it should be clear that the data subject has explicitly consented to the disclosure and any authority to act has sufficient power to cover this. It does not necessarily mean that someone who says that they are acting on someone's behalf actually is. You should check to ensure the 3rd party is legitimate.

You need to ask yourself whether there is a clear and informed 'authority to act'. Receiving a form with just a signature on does not necessarily mean that the consent for the authority to act is either informed or even genuine, as emails or signatures could be spoofed, copied etc. It is important to look into the authority to act to ensure that the data subject is fully informed and has conscious knowledge that the request is being made on their behalf. You may wish to email or telephone the data subject to validate this.

A template or basic authority to act may not be valid in itself. DSARs can often be quite privacy invasive, disclosing sensitive data about the data subject. Often the data subject may not necessarily appreciate the sensitivity or the volume of the personal data which is to be shared with the 3rd party. In such instances you may ask the data subject or the 3rd party to provide a more explicit authority to act covering this point, or alternatively, cut out the 3rd party completely and respond directly to the data subject (allowing them to choose what parts of the data they comfortably want to share with the 3rd party).

4.3 DSAR PLATFORMS

Several online platforms have recently been developed allowing data subjects to submit their request via 3rd parties. Examples of these include: TapMyData, Jumbo and Rightly. Whilst it is encouraging to see more mechanisms to allow data subjects to invoke their rights, these must be treated with a level of caution. It is important that you undergo positive identification validation of the data subject and ensure they are fully informed of what the DSAR process entails. As a data controller you may also have to do a level of due diligence to ensure you are disclosing personal data in a safe and secure manner to such platforms. You may feel it is more appropriate to first validate the legitimacy of the request from the data subject themselves and then subsequently respond directly to the data subject instead.

4. VALIDATING THE REQUESTOR CONT...

4.4 ARE THEY ACTING FOR ANOTHER AGENCY (SUCH AS THE POLICE, THE COURTS, HMRC, ETC?)

It is a challenge to provide an exhaustive guidance on the variety of circumstances surrounding the nature of requests coming from official bodies or other third parties. Detailed guidance relevant to your specific situation should be sought from a specialist prior to making any decisions. Important questions you should ask yourself or potentially the requestor are:

- Is there a provision under the Data Protection Act 2018 which may permit the disclosure in certain circumstances?
- Are there other statutory or legal provisions which support the disclosure or give public authorities powers to obtain data concerning 3rd parties? (i.e. safeguarding disclosures, DBS checks etc.)
- Is the disclosure mandated by an order of the court?
- Is it covered by a valid information sharing agreement?
- Is the disclosure necessary, proportionate, legitimate, fair etc. in the circumstances and what is the overall 'public interest'?

4.5 WHERE NO RIGHT OF ACCESS APPLIES

If you have sufficiently considered all of these points above and feel that there is no applicable right of access, then the request should be refused. You may wish to consider using the following text:

I write in connection with your request received on [DATE] seeking access to [DESCRIPTION OF THE REQUEST].

It is not possible to fulfil your request. This is because it is the company's view that the disclosure of the information sought would be prejudicial to the data protection rights of the individual concerned and would breach our obligations under the Data Protection Act 2018 and the General Data Protection Regulation.

If you feel that this is incorrect, you may wish to outline your request to [INSERT RELEVANT DEPARTMENT] for reconsideration. As part of this it is important that you clearly define any relevant rationale or legal provisions being relied upon to support this request.

5. BEGINNING TO PROCESS THE DSAR

It is important to actively manage the lifecycle of a DSAR. Logging and recording all subsequent actions and decision making is imperative in demonstrating that you have fully complied with the obligations placed upon you by virtue of the Data Protection Act 2018 and the GDPR. Such records are important in the event of a dispute with the data subject or to evidence your course of action to the Information Commissioner's Office (ICO).

5.1 LOGGING

It is recommended that you maintain a record of all requests received, date of receipt and the employees responsible for certain tasks associated with the completion of the request. Appropriate diary reminders should be diarised in calendars and the estimated resource time required allocated at an early stage to ensure the successful active management of the DSAR. A DSAR log does not have to be overly complicated, a spreadsheet would suffice, but it is important that everyone knows where the log is stored, who DSARs should be sent to and whose responsibility it is for collating, redacting and responding etc.

5.2 ACKNOWLEDGING

It is important to engage in positive communication with the data subject or the requestor (if a 3rd party) as soon as practically possible. Whilst not a mandatory requirement, an acknowledgement can clearly outline the terms of engagement and set expectations – i.e. it can define that the request is a DSAR (which may not have specifically been outlined by the requestor) and that it may take up to a month (or three months in exceptional circumstances) before a response is forthcoming. This gives the requestor confidence that their DSAR is being processed (not ignored) and could alleviate the need for them to regularly chase the company for a response, before the one-month period has expired. An example of acknowledgment wording can be found to the right:

I write in connection with your request received on [DATE] seeking access to [DESCRIPTION OF THE REQUEST].

Your request has been identified as a Data Subject Access Request (DSAR) as per the provisions of the Data Protection Act 2018 and the General Data Protection Regulation.

The timescale for complying with such a request is usually one month, however in exceptional circumstances this can be extended up to a total of three months. Should your request be delayed due to any reason, you will be notified and provided with a revised completion date.

Enquiries relating to your request, should be directed to: [INSERT POINT OF CONTACT]

5. BEGINNING TO PROCESS THE DSAR CONT...

5.3 RETRIEVING

Collating data as part of a DSAR can often be challenging due to the amount of the personal data involved or because of the manner or structure in which that data is kept. There is a high expectation on you to provide information in response to a DSAR. Extensive efforts will need to be undertaken to find and retrieve the requested information. It should however be noted that there is no obligation to create new information which does not exist. Grounds for refusing requests are only permitted whereby they are excessive or manifestly unreasonable (see Section 5.4).

If you process a large amount of personal data concerning the data subject, you can ask them to specify the information or processing activities that their request relates to before responding to the request. However, it should be noted that this will not affect the one-month timescale for responding whilst they come back to you. It is not permissible to require the requester to narrow the scope of their request, but it is ok to ask them to provide additional details that will help you to locate the data they are seeking, i.e. the likely dates when any processing may have occurred or names of the staff they have engaged with.

It should be remembered that a data subject is entitled to ask for everything you hold about them. If the data subject does not provide constructive information to assist you, you must still comply with their request by making reasonable searches for the information covered by the request. A robust records management regime should assist you in locating information efficiently.

5.4 CHARGING, EXCESSIVE AND MANIFESTLY UNFOUNDED REQUESTS

You can only charge a reasonable fee for the administrative costs of responding to a DSAR where it is manifestly unfounded, excessive, or if further copies have been requested. The introduction of the GDPR abolished the previous £10 access fee which could be charged under the previous Data Protection Act 1998. Any fees should be based upon reasonable administrative costs and the decision to charge should be notified to the data subject promptly. Work need not commence until the fee has been received.

Another option available to you is to refuse to comply with a manifestly unfounded or excessive request. The decision should be made on a case-by-case basis and your rationale for this should be clearly documented in case this needs to be demonstrated to the ICO or the courts.

Examples of requests given by the ICO which may be manifestly unfounded are:

- The individual clearly has no intention to exercise their right of access. For example an individual makes a request, but then offers to withdraw it in return for some form of benefit from the organisation
- The individual has explicitly stated, in the request itself or in other communications, that they intend to cause disruption
- The request makes unsubstantiated accusations against you or specific employees
- The individual is targeting a particular employee against whom they have some personal grudge
- The individual systematically sends different requests to you as part of a campaign, e.g. once a week, with the intention of causing disruption

5. BEGINNING TO PROCESS THE DSAR CONT...

The ICO adds that there is not a presumption that a request is manifestly unfounded simply because the individual has previously submitted requests which have been previously ruled as manifestly unfounded or excessive, or if it includes aggressive or abusive language. Each request must be judged upon its own merits. You should consider the specific situation and whether the individual genuinely wants to exercise their rights. For example, a data subject may be looking for access to their data to support or disprove a genuine grievance they may have about your company. In such instances, it would be unlikely that the request would be manifestly unfounded.

Examples of requests given by the ICO which may be excessive are:

- It repeats the substance of previous requests and a reasonable interval has not elapsed
- It overlaps with other requests

Requests are not necessarily excessive just because the individual has requested a burdensome large amount of information. As detailed above, you may wish to consider asking them for more information to help you locate the information they are specifically seeking.

If you wish to rely upon the fact that the request is manifestly unfounded or excessive, you must notify the requestor and detail the reasons why, explain their right to make a complaint to the ICO and their right to seek judicial remedy to enforce their rights. Such notifications should be sent without undue delay and within one month.

6. IDENTIFYING INFORMATION TO BE REDACTED

There will often be occasions where the provision of personal data as part of a DSAR may come into conflict with other data protection or privacy rights or potentially prejudice other legal provisions or interests. To protect such rights or interests, the information should be removed or redacted from the disclosure.

6.1 GENERAL PRINCIPLES AROUND 3RD PARTY PERSONAL DATA

There will be occasions whereby the sourcing and provision of a data subject's personal data will also include the personal data of other parties, such as family members, staff who have dealt with the data subject, individuals who have made allegations against the data subject etc. When identifying the personal data of a 3rd party, a balance should be struck between the requestor's right of access, against the data protection, privacy or any other rights of that 3rd party. You cannot automatically remove or refuse access to personal data about or sourced from a 3rd party.

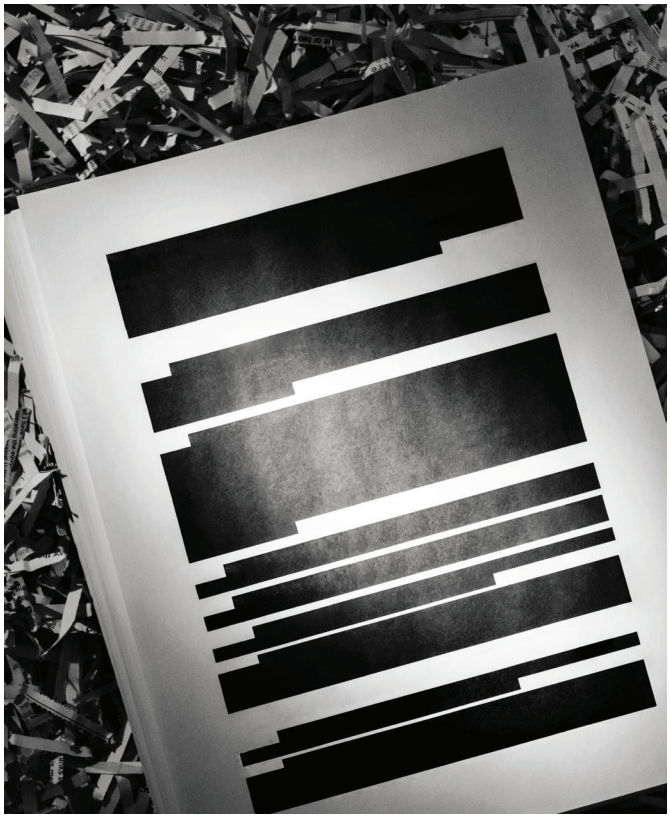
You do not have to provide information relating to 3rd parties, unless the 3rd party has consented to the disclosure (see Section 6.1.1) or it is reasonable to provide the information without that individual's consent.

The ICO adds that in determining whether it is reasonable to disclose the information, you must consider all of the relevant circumstances, including:

- The type of information that you would disclose
- Any duty of confidentiality you owe to the other individual
- Any steps you have taken to seek consent from the other individual
- Whether the other individual is capable of giving consent
- Any express refusal of consent by the other individual

Whilst it is possible on occasion to disclose information about 3rd parties, you need to determine whether this is appropriate, and this is achieved by the aforementioned balance between the respective data protection rights of access and protection.

For example, if data subject A provides a witness statement as part of data subject B's disciplinary investigation, it would not be appropriate to provide any internal analysis of data subject A's evidence to data subject B as part of a DSAR.



6. IDENTIFYING INFORMATION TO BE REDACTED CONT...

6.1.1 OBTAINING AND SEEKING CONSENT

In order to alleviate the risks associated with getting the balance incorrect, an appropriate course of action would be to seek consent from the 3rd party. If the 3rd party provides their consent to you disclosing their data, it would be reasonable to do so. However, there will often be occasions whereby it is not appropriate to seek the consent of 3rd parties:

- Where seeking consent could prejudice the data protection rights of the requestor
- Whereby subsequent harm could arise from seeking consent
- Where it is inappropriate in the circumstances to seek consent (i.e. from a victim of a crime, an estranged partner going through acrimonious divorce proceedings, an individual who does not have sufficient capacity to give consent etc.)

If you choose not to seek consent from a 3rd party, your rationale for this should be clearly documented.

Example content for a letter seeking consent can be found to the right:-

Dear [NAME],

[COMPANY] has recently received a Data Subject Access Request from a third party. Under the provisions of the Data Protection Act 2018 and the General Data Protection Regulation (GDPR) individuals have a right to access personal data relating to them. Whilst collating the relevant data, we have located the following records which relate to yourself too (a copy of which has been enclosed for your perusal).

As part of our decision-making process, we are required to balance the individual's right to a Data Subject Access Request, against any privacy or data protection rights that you may have. In responding to such a request, [COMPANY] has a duty to disclose all relevant personal data, unless an exemption or a specific overriding argument applies, such as it would breach a duty of confidence or would undermine your own data protection rights causing damage or distress. If you feel this is applicable in this case, please reply to me, outlining why you feel this is the case.

Under data protection law we are required to process a Data Subject Access Request within one month of receipt. As such, it is vitally important that you give this matter your urgent attention.

If [COMPANY] has not received any feedback from you by [GIVE TWO WEEKS], [COMPANY] will assume that you have no outstanding concerns and you are happy for [COMPANY] to make appropriate decisions around disclosing or withholding your data.

If you wish to discuss further, I am available on the following contact details:

6. IDENTIFYING INFORMATION TO BE REDACTED CONT...

6.1.2 DISCLOSING PERSONAL DATA ABOUT COLLEAGUES, STAKEHOLDERS AND PROFESSIONALS

When considering the disclosure of records relating to a data subject, they will often contain the names of colleagues or other stakeholders within them – i.e. the author of emails discussing a data subject, those who have created records about the data subjects, those from partner agencies or companies who have shared information about the data subject etc. In such instances this information has been recorded in a professional capacity and it is hard to withhold such personal data for accountability reasons. A debate between personal data and professional data will ensue. In order to reconcile whether disclosure would be fair and reasonable, the following concepts should be considered:

CONSIDERATION	EXAMPLE	OUTCOME
Does the content relate to special characteristic personal data? (i.e. medical or health conditions, ethnicity, criminal offences etc.).	An email from employee A to their manager explaining that they cannot visit the data subject as they are having a pregnancy scan.	There would be an expectation this would primarily constitute personal data relevant to the employee, not necessarily that of the data subject and would be redacted.
Would the disclosure have unjustified significant consequences on the professional?	An email from employee B (an undercover investigator) outlining the evidence they have captured about the data subject.	If the investigation has been concluded and there is no prejudicial effect, it may be appropriate to share the content with the data subject. However, it may be appropriate to redact the undercover investigator's name to preserve their covert role or to protect their identity in the event that the data subject may seek revenge.
Is there a reasonable expectation that their personal data will be released? You should consider whether it relates to the personal data in a professional capacity, their seniority and the public facing nature of their role.	An email from the HR Director containing interview feedback concerning a potential candidate.	There is a reasonable expectation that those making decisions about individuals in key roles should be accountable and open to scrutiny. A potential candidate has a legitimate expectation that they should be able to receive constructive feedback about their interview. There would be less of an expectation for the disclosure of the name of the reception staff who welcomed the candidate into the building.

Even though disclosure may cause distress, this does not necessarily mean that disclosure of the data of those in a professional capacity would be unfair. Those making decisions in respect of DSARs need to balance the right of access alongside the legitimate privacy or data protection expectations of professionals. Personal data relating to professionals routinely shared as part of everyday business (i.e. the names of employees in public facing roles, work/business contact details, professional opinions etc.) are unlikely to attract a level of consequence if the data was disclosed as part of a DSAR. However, as in all instances, this should be judged upon a case-by-case determination.

The same principles apply in respect of those which do not work for your company, but in determining any level of risk, you may wish to consult with these 3rd parties to present their own evidence for you to consider.

6. IDENTIFYING INFORMATION TO BE REDACTED CONT...

6.2 IDENTIFYING CONFIDENTIAL CONTENT

As you will have seen so far, the right of access under a DSAR does not necessarily trump other rights or interests. Another example of this is where information is deemed to be confidential, it has been given in confidence or attracts a duty of confidence. Simply adding a CONFIDENTIAL banner to a document or marking an email as such, does not necessarily mean that the content is confidential. A case-by-case assessment on the content should be made. For something to be confidential, it must have the quality of confidence about it and the relationship imparts a duty of confidence (i.e. informant/investigator, doctor/patient, solicitor/client etc.)

Examples of confidential content you may wish to withhold are:

- Details of information originating for confidential complainant which would allow the identification of the source
- Information which may jeopardise commercial confidences (such as trade secrets, commercial rates, intellectual property etc.)
- Information gathered as part of a confidential relationship (such as doctor and patient).
- Information covered as part of a non-disclosure agreement

Disclosure of such information (even as part of a DSAR response) could result in the individual or company whose rights have been compromised having a claim against the company, unless there is the overriding public interest in the disclosure of the information. Examples where this may be applicable is where the content could:

- Prevent the harming of other individuals
- Assist the prevention or detection of serious crime
- Be proven to be manifestly or mischievously untrue

If there is no overriding public interest which can be evidenced, then this must be redacted within the DSAR disclosure.

6. IDENTIFYING INFORMATION TO BE REDACTED CONT...

6.3 AVAILABLE EXEMPTIONS

The GDPR has empowered EU Member States to create a number of exemptions from the rights available to data subjects. These have been enacted in Schedule 2 of the Data Protection Act 2018. A Data Controller can restrict access to data subject rights including DSARs whereby it is necessary to safeguard:

- Crime and taxation
- Crime and taxation risk assessments
- Information required to be disclosed by law or in connection with legal proceedings
- Legal professional privilege
- Self-incrimination
- Disclosure prohibited or restricted by an enactment
- Immigration
- Functions designed to protect the public
- Audit functions
- Bank of England functions
- Regulatory functions relating to legal services, the health service and children's services
- Other regulatory functions
- Parliamentary privilege
- Judicial appointments, independence and proceedings
- Crown honours, dignities and appointments
- Journalism, academia, art and literature
- Research and statistics
- Archiving in the public interest
- Health data
- Social work data
- Education data
- Child abuse data
- Corporate finance
- Management forecasts
- Negotiations
- Confidential references
- Exam scripts and exam marks

Whilst not defined as exemptions, the ICO adds that the following purposes also provide an exception to provision of information for the DSAR:

- Personal or household activities (as personal data processed in the course of a purely personal or household activity, with no connection to a professional or commercial activity, is outside the GDPR's scope)
- Law enforcement
- Safeguarding national security or defence

As part of a brief guide it is not possible for this document to go into each of these in any degree of detail. Examples of their applicability can be found on the ICO's website. However, the key component to understand is that the withholding of information as part of the DSAR is necessary to safeguard those purposes. Demonstrating the necessity will be critical for the successful application of an exemption. Each application will need to be evidenced, along with your documented rationale for doing so, as this may need to be demonstrated to the ICO or the courts.

As part of gathering evidence you may wish to consult with the affected bodies to provide support in this pursuit. For example, it may be appropriate to consult with the police to determine the extent to which the disclosure of shared intelligence may have upon their impact upon the ability to apprehend an offender.

An exemption is extremely unlikely to attract a blanket exemption to the full content of a DSAR and focus should be placed on those sections of the records which prejudice those specific safeguards.

7. PRACTICAL CONSIDERATIONS

7.1 HOW TO REDACT

Redaction can be performed in a number of ways and your options may be dictated by your software, your stationery, your printing capabilities or the desires of the requestor. Redactions can be completed electronically or by hand.

One of the most adopted methods is by using the full version of Adobe Acrobat (not just Adobe Reader). There are other tools on the market which are similar. Adobe allows for content to be scanned by Optical Character Recognition (OCR), allowing for text searching and automatic redaction, but it also gives you a tool to redact content manually, as shown in **this YouTube video**. Redaction within Microsoft Word is not recommended as the content can be copied and pasted with formatting removed allowing the original content to be revealed.

Another secure method is to undertake the redaction manually by hand. Before undertaking redacting activity, it is important that your disclosure bundle is printed out single sided. Manual redaction can be completed by clearly colouring over or marking over the protected content, preferably with a straight line. You do not need to be concerned by the fact that the marked over content can potentially be read through on the flip side, as this can be alleviated on completion by photocopying or scanning the disclosure bundle on the darkest brightness setting and sending the output instead.

7.2 WATERMARKING

It is recommended that a disclosure is accompanied with a watermark prior to release. This allows you to distinguish between original documents circulating within your company, against that of the copy which is provided to the requestor. If the records are provided in hard copy form in an uncontrolled manner to the requestor, in the event of grievance, it is not beyond the realms of possibility that the requestor could wilfully release or dispose of their disclosure in an insecure manner. Without any clear watermarking to distinguish the requestor copy from your own internal copies, it would not be possible to determine who is responsible for any data breaches associated with this information. The watermark can also be used to reinforce additional messages such as a copyright warning if necessary. The following **instructional video** from YouTube demonstrates how watermarks can be applied in Adobe Acrobat.

7.3 PREPARING IN THE FORMAT REQUESTED

You may wish to seek the preference of the requestor prior to collating their response and sending it to them. Generally, if an individual made their request electronically, then it should be provided in a commonly used electronic format (unless they specify otherwise). You should also be mindful of the data subject's rights around **data portability** should that be their ultimate aim.

8. RESPONDING

8.1 COVERING LETTERS

It is good practice to include a covering letter or accompanying explanatory material as part of your DSAR response. It must not be forgotten that the right of access does not just cover the provision of information, it also contains confirmation of the details and nature of processing, which can be included in your covering letter.

If refusing the request in its entirety on excessive or manifestly unfounded grounds, you must explain your reasons for refusal, the right to complain to the ICO and the ability to enforce rights through judicial remedy.

If information has been supplied and is unintelligible, you are required to provide the information in a concise, transparent, intelligible and easily accessible form, using clear and plain language so that the content could be understood by the average person. Where this is provided to a child, it should be understandable to that child. For example, if you have a traffic light scheme for grading the attendance records for staff or a warning marker system, it is expected that you will provide clarity as to what such gradings or marks mean.

If you have redacted information as part of the disclosure it is vitally important that you explain the rationale for this and any appropriate exemptions used. Whilst it may not be possible to detail the reasoning behind each individual redaction to the data subject, you should still be expected to explain the purpose for which the redactions have applied. It should however be noted that for your own benefit you should maintain records of your own decision-making as to why a redaction has been necessary in case of dispute. You should always take care to ensure when explaining the existence of an exemption to the requestor that it does not undermine the issue you are safeguarding. For example, you may not be able to share that a law enforcement or national security exemption may be applicable if the individual is subject to covert surveillance as this is likely to undermine the investigation.

Whilst it is not possible to provide a template to cover all circumstances, the template overleaf provides you with an indication of the nature of the content that you should be including within a covering letter.

8. RESPONDING CONT...

Dear

Data Subject Access Request – Reference:

I write in connection with your request received on [DATE] seeking access to [DESCRIPTION OF THE REQUEST].

Your request has been considered in line with the Data Protection Act 2018 and the General Data Protection Regulation, and the personal data you are entitled to has been included with this letter. Additional to the provision of your personal data, I can confirm that [Company] processes your personal data and for more details surrounding the purposes and scope of this can be found within our Privacy Notice [PROVIDE LINK OR COPY OF PRIVACY NOTICE].

You may note that certain parts of your disclosure have been redacted (i.e. removed with black marks), this is because it contains...

[LIST OF EXEMPTIONS:

Information relating to 3rd parties:

Under the right of access, Data Subjects are only entitled to their own personal data and not necessarily that relating to any 3rd parties. As part of providing information we have had to consider your right of access and balance that against any other rights that other individuals such as protecting their own data protection or privacy rights.

Information provided in confidence:

There will often be occasions whereby information is provided in confidence to the company and release of such would undermine that duty of confidence potentially resulting in legal consequences for the company. Furthermore, it is important that such confidences are respected and that individuals can share matters with the company in confidence without fear that their confidence will be breached. Please rest assured that what we can share in respect of these instances will have been shared or anonymised appropriately.

I hope that you find the enclosed information useful. [COMPANY] now consider your request fulfilled and the matter to be closed. Should you feel this is not the case, in the first instance please let me know. If you remain dissatisfied following this, please note that you have the right to raise the issue with the Information Commissioner's Office (ICO), who can be contacted by the following methods - ***https://ico.org.uk/global/contact-us****/. You also may wish to seek to enforce your rights through the Courts.*

If your concerns related to procedural matters rather than the provision of information, please can I politely suggest that such matters are taken up with the relevant departments or via our complaints processes.

8. RESPONDING CONT...

8.2 SECURE DELIVERY

Where appropriate your method of delivery should reflect that choice outlined by the requestor. It is imperative whatever method you choose to use is secure.

8.2.1 POST

If the response is to be communicated in hard copy format, then a decision on the delivery method should be based around the sensitivities contained within the disclosure. You may be comfortable sending the content out in normal post. However, in cases whereby the disclosure reveals content that is particularly sensitive and contains special category data, you may wish to choose a recorded or signed-for postal or courier service. Alternatively, if you have a good rapport with the requestor and they are regularly visited as part of client or customer review meetings, you may choose for their regular point of contact (i.e. a caseworker who normally does home visits) to drop off the completed disclosure.

8.2.2 ELECTRONIC MEANS

Completed disclosures can be transferred securely by several means. These include secure email, secure file transfer or encrypted media. Prior to sending a response, it is recommended that the disclosure be locked down in a secure tamper-proof format, ensuring that the original cannot be tampered with (i.e. removing of the secure watermark, allowing the recipient to edit content to tell their own narrative etc.). In terms of emailing the disclosure, the preferred option would be via a secure email provider. If sending the disclosure by encrypted media or by file transfer, the disclosure should be passworded to an encryption standard of 256-bit AES prior to sending. It is important that any explanatory material detailing how to access the disclosure does not contain the password to access the file and this is sent via other means, i.e. text message or a follow-up telephone call.

8.3 REQUEST CLOSURE

After the DSAR has been responded to it is important that you close the case on any internal registers or databases you have. This should contain the date the DSAR was responded to and a comprehensive list of actions and any decisions made. This allows you to evidence your compliance in the event of a dispute but also ensures you maintain a register of what information has been disclosed and who to.

APPENDIX A: DSAR PROGESS CHECKLIST

This checklist serves as a handy prompt to walk you through the various steps that you need to consider whilst processing a DSAR. Feel free to print this out and tick off each step as you go along to ensure you have fully completed the DSAR.

- ☐ Logged the request
- ☐ Validated the identity of the requestor (or establish that a sufficient authority to act exists)
- ☐ Established the type and scope of the request (seek clarity if needed)
- ☐ Acknowledged the request in writing
- ☐ Performed searches and/or contacted relevant departments to undertake searches
- ☐ Considered the application of any exemptions
- ☐ Considered whether any 3rd party personal data needed redaction (Note: you may need to seek consent)
- ☐ Watermarked the response
- ☐ Produced a covering letter
- ☐ Sent response securely
- ☐ Recorded our decision making and closed on the DSAR Log

APPENDIX B: JOINT CONTROLLERS

Due to the nature of joint data controllers, data subjects will need to know who they can send a DSAR to.

It should be made clear within the relevant privacy notice or documentation how a data subject can submit a DSAR and to whom it should be addressed. If a DSAR is received from one of the joint data controllers, the other data controller should be informed about the request. If it transpires both controllers are affected by the DSAR, a coordination effort will be needed to fulfil the request.

The rules and requirements of a DSAR still apply as they are and there are no special exemptions or differing rules for joint data controllers. It is therefore recommended the joint data controllers collaborate to ensure all relevant data is gathered and this guidance is followed.

APPENDIX C: PROCESSORS

The GDPR states data processors must help the data controller carry out any data subject rights including DSARs. This should also be mirrored in the relevant agreement with them.

If a data processor does receive a DSAR, that request should immediately be sent to the data controller, who should carry out the authenticity check and communicate the receipt of the request received by the data processor with the data subject. The data processor may be able to do this on behalf of the data controller but should be agreed to without further delay.

Following this the data processor must work with the data controller in retrieving all relevant information requested and carrying out actions as described above. When the DSAR is ready to be sent out on the approval of a data controller, the data processor can send the information as requested or it can be sent out by the data controller.

THE DPO CENTRE:
DSAR RESPONSE SERVICE

Avoid the many challenges associated with responding to your organisation's DSAR requests by outsourcing them to The DPO Centre's dedicated DSAR team. Our team provides the experience, knowledge and tools to respond effectively and within the stipulated timeframes, leaving you free to concentrate your time more productively elsewhere.

HOW THE SERVICE WORKS

The service is delivered on an ad hoc 'pay as you go' basis, where you outsource all, some, or just occasional DSARs to us as required. We can take care of the full 'A-Z' of the DSAR response process, provide just an advisory and oversight service, or perform only certain aspects, such as redaction.

OBJECTIVES

- Enable you to respond appropriately and in a timely manner
- Remove the burden and distraction associated with DSAR responses
- Significantly reduce the risk of compliance failure and Regulator scrutiny
- Assist in improving data subject trust and de-escalating contentious situations

APPROACH

- Provide model template responses for communicating with data subjects
- Provide guidance around scope defining and conducting database searches
- Conduct full de-scoping and redaction exercises
- Complete delivery of response to data subjects
- Handle all correspondence with the relevant supervisory authority

OUTCOMES

- Immediate access to Subject Matter Experts
- Peace of mind that you are working with one of the largest, most established data protection providers available
- Removal of the distractions and costs associated with training and managing internal resources to respond
- Implementation of established and verified response processes and standards
- Substantial reduction in regulatory and reputational risk

By engaging with our DSAR Response service, you will have the peace of mind that an expert team is there to support you. If you would like to know more about how we can help, please contact us.

HOW CAN THE DPO CENTRE HELP?

The DPO Centre is an organisation consisting of a team of full-time and permanently employed DPOs located throughout the UK. Every member of this team is an experienced DPO who is knowledgeable and highly adaptable, so can deliver the exact level of support required and in the precise manner you require it.

This may be to assist you with one-off projects, such as a data protection audit or a complex DSAR request, or to provide support conducting DPIAs. Furthermore we can provide interim support to cover sickness, maternity and employment gaps and can deliver ongoing assistance, as your designated DPO, taking ownership of the day-to-day responsibility for the role, delivered based on the exact level of resource required to meet your evolving needs.

To find out more about our service visit:-

website

hello@dpocentre.com

0203 797 1289

Amsterdam · Dublin · London · New York · Toronto
+44 (0) 203 797 1289
hello@dpocentre.com
www.dpocentre.com

04-2025