# DSAR Guidance Tool – User Guide

**Introduction:**

The following guidance is directed at Data Protection Officers or staff performing a similar function within their organisation (collectively referred to as the "DPO" for the purposes of this guidance), to assist in the facilitation of Data Subject Access Requests ("DSAR").

The following tips are broken down into the stages relevant to managing a DSAR.

This should be used alongside the Authority's Guidance for Controllers, which drills down further into Data Protection legislation and the DSAR process.

We have also developed the '**DSAR Manager**': a spreadsheet tool designed to support controllers and DPOs in managing their DSARs, ensuring the necessary detail is recorded and accurate.

Properly maintained records regarding DSARs is an invaluable tool both **internally** (administrative, statistical, business continuity etc) and **externally** (communicating with the data subject or the Authority).

I always recommend that detailed records are maintained noting the controller's decisions made during the DSAR process and any other important information that may have impacted the request or otherwise be pertinent.

The DSAR Manager is a great location to record this information and should be supported with a structured filing system, using standardised naming conventions where you can save any related correspondence and supporting documentation.

This is NOT a mandatory tool; however, it may be useful to you in processing a DSAR.

| (0) Front Page: | |
|---|---|
| **Easy reference** | The purpose of this page is to act as a quick reference point, summarising the key information*, such as the DSAR due date. This can be helpful when managing multiple DSARs with varying deadlines and ensures all related material is recorded appropriately under a unique DSAR reference number (generated internally by the organisation).<br><br>**Note - under the Law, the Data Protection Officer is an independent function therefore you will need a separate, suitably senior individual to represent the controller and sign-off on any relevant decisions, including disclosure. Ensure this individual is also recorded on this page.* |
| **Keeping records** | You will note that the DSAR Manager has a free-text box on every tab for additional considerations, notes and comments. Any factors relevant to a DSAR that do not fit elsewhere should be recorded here.<br><br>An ongoing theme when handling DSARs is the value of maintaining detailed notes. There are no rules for what goes in these boxes so utilise them however suits you and the organisation best. This further supports the reference function of the spreadsheet and can also provide necessary context to the controller and the Authority should the matter be investigated. |

| (1) Acknowledge: | |
|---|---|
| **One calendar month and notification** | A controller has <u>one calendar month</u> to comply with a DSAR, NOT 30 days. This means if a request comes in on 1 May it will be due **1 June***.<br><br>In practice, this can feel like a very short timeframe and therefore it is recommended to notify the relevant individuals within the organisation as <u>early as possible</u>.<br><br>This includes:<br>• The DPO (if they did not receive the DSAR directly)<br>• The controller's representative<br>• The relevant staff or departments likely to hold the requested information (*see Collation tab of DSAR Manager*) |

| | |
|---|---|
| | It may be that you have not confirmed whether the request is, in fact, a DSAR or are awaiting verification of the requestor's identity. However, this early notification can still be valuable and ensures you can respond promptly once the necessary information has been received.<br><br>Failing to action early can cause a domino effect of delays, resulting in a dramatically reduced period in which to consider the collated material and ultimately meet the deadline.<br><br><u>Don't be afraid to start the process</u>.<br><br>**Note - the DSAR Manager will automate the due date based on the date of receipt/verification. You can also use it to determine the due date should the controller apply a one- or two-month extension.*|
| **Supporting officers** | For large organisations, it may be helpful to establish supporting officers within certain departments who can act as both your contact point as well as facilitating the collation of material from staff within that department. With some basic training, this can serve a dual purpose:<br><br>(i) Increasing general data protection awareness.<br>(ii) Allowing for early identification of DSARs and breaches within that department.|
| **Early contact with requestor** | Make sure to engage with the data subject at the earliest opportunity*, confirming receipt and clarifying any queries the controller may have, such as the scope of the request (any time period given, relevant info, relevant departments).<br><br>Requestors often hold a negative perception of the receiving organisation therefore early communication, to better understand the DSAR, can help build trust and demonstrate the organisation's transparency. When requestors feel "left in the dark" or "forgotten" trust quickly erodes, often leading to a protracted, more adversarial and ultimately costly experience (both in time and resources). It also increases the likelihood that a formal complaint is made to the Authority.<br><br>**Note - questions to the requestor, clarifying scope etc, do not pause the DSAR, hence why early engagement and notification to the relevant areas/departments can be so valuable.*|
| **Verifying identity** | You may find that you are unsure of the identity of the requestor and so need to take steps to verify their identity. As a result, the clock will not have started yet, however, be cautious not to abuse this part of the process by delaying|

| | |
|---|---|
| | communications with the requestor. Responses should be prompt and with a view to facilitating the DSAR as soon as is practicable.<br><br>Any unnecessary delays will not be viewed positively either by the requestor or the Authority and can ultimately lead to a formal complaint. |
| **Other ongoing processes** | It is important to note that alternative processes, through which a requestor would ultimately receive some or all the requested information, do NOT automatically negate a DSAR. A good example of this is an Employment Tribunal. The Law still requires you to proceed with the DSAR process.<br><br>This is not to say there are no instances where an alternate process would overrule the right to access e.g. law enforcement or regulatory investigations. You will need to ensure you are therefore aware of any ongoing matters and whether they would justify the application of an exemption under the Law. |

| **(2) Collation:** | |
|---|---|
| **P&Ps** | Alongside the review stage, collation can be the most time-consuming part of a DSAR. It can therefore be beneficial for an organisation to implement internal policies and procedures ("P&Ps") that inform general employees of the typical DSAR process, list all applicable systems and place requirements on staff and departments to support the collation of materials.<br><br>A requestor will often not be aware of who to direct their request to therefore informing staff in your organisation of the DSAR process and its requirements, via these P&Ps, ensures you are notified as soon as practicable should an employee receive a potential DSAR. It also means they can provide valuable and timely assistance. |
| **Avoid unnecessary delays** | Contributing staff and/or departments may see the statutory deadline as solely for the collation process, not realising the importance of the subsequent review stage. This can lead to a de-prioritisation and unnecessary delays, which may ultimately impact your ability to disclose on time. |

| | |
|---|---|
| | Do not be afraid to implement organisation-wide guidelines such as internal deadlines for collating personal data and providing it to the DPO. These deadlines can be incorporated into the P&Ps and sign-posted in staff inputs, inductions etc. |
| **Addressing scope** | It is important to cast the net wide when considering the people and systems that may be captured by an individual's DSAR. Organisations can often fall foul by being overly reliant on a single system and not considering other information available to them elsewhere such as through applications like Microsoft Teams, staff Outlook accounts, archived records or physical documentation.<br><br>Communicate with the requestor to ensure you fully understand what they are requesting and, where necessary, help them understand what you hold. *<br><br>**Note - The requestor is not legally required to reduce the scope of their request. They will also not be privy to the ins and outs of a large organisation's multiple systems. Do not assume just because the requestor has not explicitly referenced a specific system or area that is not captured by their request.*<br><br>*Requests can also include information previously sent to the requestor (emails, letters etc). The fact they have previously received them does not exclude that information from the DSAR process.* |
| **Identify sources of personal data** | Even when following internal guidance, exercise judgement and don't limit yourself in terms of potential data sources:<br>• What is the information being requested?<br>• Is it held by a third-party provider (IT / HR for example)?<br>• Do you allow for the use of work mobile devices?<br>• Do you allow use of personal devices for work purposes and is there an indication they hold relevant information?<br>• Is it archived?<br>• Have you considered physical storage?<br>• Individual consultants?<br>• Pseudonymous data*<br><br>**Note - just because the requestor is not named does not necessarily mean it is not their personal data. If your organisation has the ability to identify the requestor through the information provided, then it is likely their personal data. A good example of this are unique customer reference numbers.* |

| | |
|---|---|
| **Data Inventory** | The Authority provides templates to assist controllers in complying with the Law - Templates · ODPA. One of these is the 'Record of Processing Activities', which lists the information controllers are legally required to record. It can also serve a dual purpose within the organisation as a data map which you can reference to better understand the various types of personal data processed by your organisation and where this is located.<br><br>The template is flexible and can be tailored to suit any organisation size (e.g. additional columns to specify departments, supporting officers etc).<br><br>If available, refer to this as early as possible; it will help direct you to the appropriate areas, systems and people that will hold the requestor's personal data. |
| **Search terms** | It is likely that, to perform an effective search, you or a supporting officer will need to implement search terms*. These will be informed by several factors such as the organisation's relationship with the requestor (employee, customer etc) as well as how you record their personal data.<br><br>Whatever search terms you use you must show they were reasonable considering the systems and processes in place. Do not forget unique IDs or reference numbers that apply to the requestor.<br><br>Additionally, do not hesitate to liaise with relevant staff or departments within your organisation for their input. They may be able to provide insight into alternative names, nicknames, reference numbers etc that you would otherwise miss. They will also likely have specific knowledge of their systems and how to best structure a search term.<br><br>For large organisations it can be more practical to request each department or operator establish the appropriate search terms themselves, based on their understanding of their area. You can still provide some guidance based on the information provided by the requestor and must ensure that the relevant department still records the terms used and the rationale for them.<br><br>**Note - requestors may often suggest their own search terms. You are not required to use these, but they may be helpful in highlighting terms you would otherwise not consider e.g. nicknames. Consider the requestor's suggestions carefully and incorporate where/if reasonable.* |
| **Recording negatives** | There may be instances where a department or member of staff responds confirming they hold NO data on the requestor. If this occurs, it is still important to record that result, demonstrating that the enquiry was conducted*.<br><br>**Note - The "Collation" tab of the DSAR Manager includes a column for noting nil returns.* |

| (3) Review: | |
|---|---|
| **References to other data** | In many circumstances, while reviewing information provided by supporting officers, you will identify references to other documents or information elsewhere. The most common example of this is an email showing an attachment, which was not provided in the pack, or referencing a relevant meeting that you would expect to have minutes. Ensure you chase these up when identified as the requestor may be entitled to the personal data therein and pick up on this when they read through the response. |
| **Transparency in redactions** | Whilst the requestor may not be entitled to all information within certain documents, it is always worth considering transparency. When looking at an email chain, it may be beneficial to disclose the departments in the signoffs and the tail of email addresses e.g. @odpa.gg*.<br><br>This avoids unnecessarily identifying any third parties but at the same time makes it clear to the requestor where the email originated and whether it was an internal or external email.<br><br>Consideration should also be given to disclosing names of senior staff/decision makers. The Authority already provides guidance on this (linked above).<br><br>**Note - there may be cases in which disclosing a department/team risks disclosing the identity of the sender e.g. where the team is relatively small and the requestor has sufficient knowledge to identify the individual based on the context of the email. You should take these factors into consideration when determining what would be appropriate from a transparency perspective.* |
| **Redaction tools** | You do not need a particularly fancy tool to perform redactions. A lot of PDF editors both allow you to compile multiple documents and provide a redaction function to permanently remove selected information. They typically allow transparent "provisional redactions" to be applied, meaning multiple parties within your organisation can review the information prior to finalising.<br><br>It is important, however, to ensure that whatever method you use is effective, irreversible (by the requestor, once finalised) and not overly onerous on the organisation.<br><br>Manual methods, for example, can be very tedious e.g. requiring multiple layers of Tippex or that you print out documents, redact them and scan them back in (even then, it may be possible to identify manually redacted |

| | |
|---|---|
| | information). Having multiple stages to the redaction process means more room for error and should ideally be avoided.<br><br>Whatever method you settle on it is recommended to retain two final copies of the DSAR pack:<br>• One version with the finalised (irreversible) redactions, disclosed to the requestor<br>• One version including the provisional redactions only + any withheld material (partial or full)<br><br>It can prove exceedingly difficult to later understand the rationale for any final redactions, both for the Authority and the controller, without the second version. |
| **Exemptions** | Just because you can apply an exemption does not mean you have to*. Properly consider what exceptions or exemptions you choose to utilise and ensure the rationale for doing so is recorded (you can use the relevant section of the "Review" tab in the DSAR Manager to log this).<br><br>**Note - Remember this rule: if uncertain whether to exempt or not, the default position should be transparency. Transparency helps engender trust in organisations.* |

| **(4) Disclosure:** | |
|---|---|
| **Have you applied exemptions?** | For the most part, you are required to advise requestors of exemptions that have been applied to the material they disclose. This also helps the requestor understand why a document may appear overly redacted and avoid a complaint. There are **limited exceptions** to this requirement where disclosure would prejudice the purpose of redacting that information in the first place – further info on exemptions can be found here - Exemptions · ODPA. |
| **Secure disclosure** | Disclosure packs can be large and full of sensitive information. You should ensure, whether physically or electronically, that disclosure is made securely. This will depend on the method, but consideration should be given to encryption, secure file sharing and tracked post. You do not want a personal data breach at the final hurdle. |
| **Layout** | Make the effort to disclose the requested material in an intelligible format. Properly date ordering the material or even using tabs/contents pages can help the requestor understand the material in front of them, which can otherwise be very difficult, if heavily redacted. This reduces the risk of the requestor raising concerns or accusing the controller of withholding personal data from them. |

| | |
|---|---|
| **Extensions** | You should make every reasonable effort to meet the normal statutory timelines.<br><br>As per our guidance, if applying an extension, you should ensure you notify an individual of that extension as soon as possible. This does not necessarily mean informing them the day you receive the request.<br><br>The decision to apply an extension should be informed and based on the circumstances of the specific request. It often reflects on the controller well if they have made attempts to facilitate the request as best they can and in doing so identified the need for an extension. Conversely, this does not mean notifying them on the day of disclosure is appropriate.<br><br>Proper communication with any supporting officers or departments can help you establish whether an extension is required (and appropriate) at a suitably early stage. You should consider all the factors available and utilise the input from your colleagues/experts to ensure that an extension is suitably justified – see our DSAR guidance for further information.<br><br>Should the decision be made to apply an extension, whether it be one month or two, it should be made clear to the requestor that efforts will be made to disclose prior to this date, if possible. This helps demonstrate a proportionate response and avoids appearing to the requestor as a delay tactic. |

| **(5) Post-disclosure:** | |
|---|---|
| **Don't be afraid to answer their queries** | Requestors will often come back after receiving their disclosure pack with more queries and concerns. Where possible, do your best to facilitate these. Large disclosure packs are often confusing and hard to decipher and any additional information you can provide will help reduce the risk of further complaints or DSARs.<br><br>The "Post-disclosure" tab of the DSAR Manager provides a log for recording these enquiries. |
| **More DSARs** | It is not unusual for a requestor to make further DSARs after receiving the initial disclosure pack. It is important that, if this happens, the controller's walls do not come down. The requestor is only entitled to personal data processed up to the point they made their request therefore there is often further information processed after that point which they |

| | |
|---|---|
| | will not have received. At the very least there will likely be information generated for the purpose of facilitating the previous DSAR. However, it is also possible you have engaged with the individual for other reasons, such as:<br><br>• Standard customer interactions (purchases, enquiries etc)<br>• Alternate processes (Employment tribunals, complaints etc)<br>• Correspondence regarding the DSAR<br><br><u>The fact the requestor has previously submitted a DSAR does not necessarily restrict them from submitting future requests.</u> |
| **Learn from the process** | Organisations vary considerably in the information they process and how they process it. How you handle a DSAR can also vary, and you may find solutions to specific problems presented during the process. Where these learning opportunities present themselves make sure to record them appropriately and take steps to update the relevant policy(ies). This will ensure future DSARs go much more smoothly and are less burdensome on you, your organisation and its staff. |