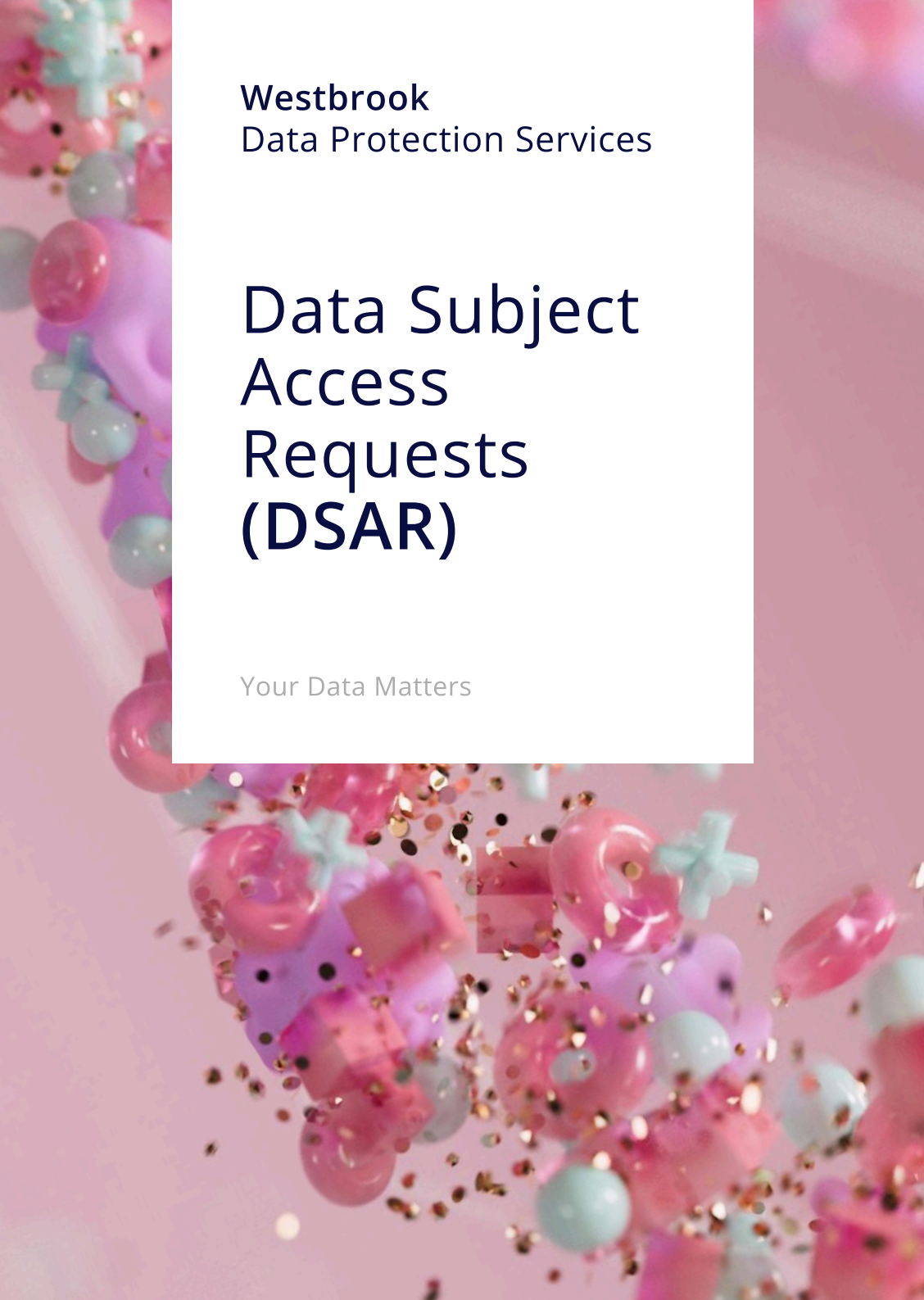


Westbrook
Data Protection Services

Data Subject Access Requests **(DSAR)**

Your Data Matters

A Data Subject Access Request (DSAR) is a request made by an individual to an organisation for access to the personal data that the organisation holds about them. This is a right granted under data protection laws, such as the Data Protection Act 2018 in the UK and the General Data Protection Regulation (GDPR) in the European Union.

What is a Data Subject Access Request?

The right of access, commonly known as a subject access request (DSAR), gives individuals the right to access personal information held about them by an organisation. A growing awareness of data protection rights is leading to an increase in DSARs.

When an organisation receives a DSAR, there is a one-month deadline to respond and failure to meet this timeline is a breach of data protection law. However, if certain criteria are met, a two-month extension can be relied upon. The Information Commissioner's Office (ICO) sets out detailed criteria for when this two-month extension may be applied.

In most instances, the one-month deadline applies and there is a need to respond quickly to meet this statutory time limit. Failure to do so may result in complaints to the ICO which could lead to correspondence from the ICO, enquiring into your organisation's processes for handling DSARs and requesting follow-up action to remedy any shortcomings. Organisations that repeatedly fail to comply with data protection laws can face enforcement action, including fines.

Recognising a DSAR

Recognising that you have received a DSAR is important, as the request may not be formally identified as a subject access request. Requests need to be correctly logged and subject to an established process. Employees should therefore be trained in how to recognise DSARs and understand what internal procedure to follow when they are received.

Example
An individual calls the water company to request a copy of their personal data. The company representative incorrectly informs them that such requests cannot be processed over the phone and suggests checking their account details online.

Instead, the representative should have recorded the individual's details and set the DSAR in motion in accordance with the company procedure for handling DSARs.

Example
A local authority receives a letter from a council tax payer requesting a copy of any information the authority holds about a dispute over his eligibility for a discount. The letter states it is a 'freedom of information request'. It is clear that the request concerns the individual's own personal data and the local authority should treat it as a subject access request.

From the Information Commissioners Office

A common channel for the receipt of DSARs is a dedicated email address established for the purpose of receiving requests. The dedicated email address is usually found in the organisation's privacy policy and all DSARs will be directed via this route.

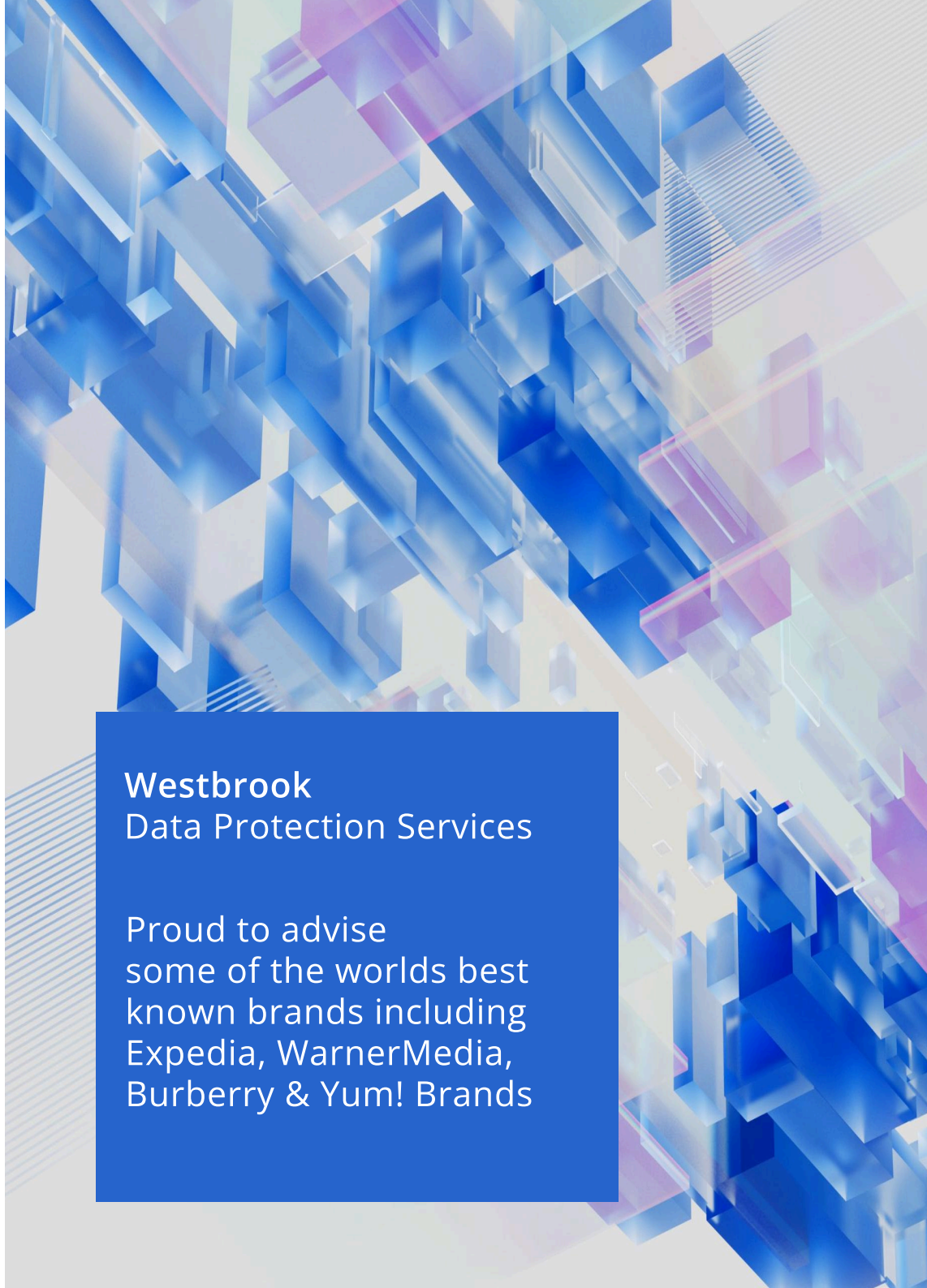
Getting the process right

Organisations that are more accustomed to receiving large volumes of DSARs will typically have an established process for handling them. However, smaller or medium-sized enterprises might be caught off guard without a clear process in place and may be ill-equipped to comply with data protection regulations.

The first challenge is understanding what information you need to provide to the individual making the request. This will partly depend on the request itself. If the request is particularly broad, it is worth asking the individual if the timeframe and/or the scope can be clarified, but you cannot put pressure on them to do this and they do not have to.

In addition to clarifying the timeframe and scope, effort should be made to carry out appropriate identity checks to ensure the person making the request is who they claim they are. During this time, the one-month countdown would pause, called stopping the clock, until the identity information and any other requested information has been received, at which point the clock would resume.

The information requested could be contained in one or more sources but will commonly include things such as emails or records of conversations from your virtual workplace, such as Microsoft Teams, for example. You need to identify the tools to search and select the appropriate search terms, depending on the nature of the request. The search will likely return a large number of documents and the next step is to review this information to determine what you are required to disclose under the DSAR.



The 5 Stage Process

The subject access request process can be broken down into five key stages, as described below:

Stage 1 - During the first stage, the search terms need to be established and the search conducted. Depending on the nature of the request, this may return a large volume of documents.

Stage 2 - The documents returned by the search will need to be reviewed in order to establish what information needs to be provided to the individual. During the initial review round, discard anything that is not personal data of the individual. It is important to understand that the right to subject access is limited only to personal data of the requesting individual.

Stage 3 - The third stage involves the removal of information about third parties, for example other people's names, or information that would easily identify other people, unless you have their consent. This information would usually be redacted.

Stage 4 - The fourth stage considers the possible application of exemptions. Determining whether these apply is something that requires technical legal expertise. If it is established that an exemption applies, you can redact or not supply the information, but you are required to provide an explanation of which information has been withheld and why you have determined the exemption applies.

Stage 5 - Once the information is ready to be sent to the individual, it should be indexed and sent securely with the password sent via a different communication channel. If hard copies of the information are being sent by post or courier, select a tracked service and consider dividing the documents into several packages to reduce damage limitation should there be any loss during transit.

The Two Month Extension

The two month extension may apply in cases where a subject access request is deemed to be complex. The ICO sets out the criteria applicable to ascertaining whether a DSAR is complex and thereby subject to the two month extension.

The criteria are as follows:

- Technical difficulties in retrieving the information – for example if data is electronically archived.
- Applying an exemption that involves large volumes of particularly sensitive information.
- Clarifying potential issues around disclosing information about a child to a legal guardian.
- Any specialist work involved in obtaining the information or communicating it in an intelligible form.
- Clarifying potential confidentiality issues around the disclosure of sensitive medical information to an authorised third party.

Tip
It is worth nothing that retention periods for financial data are generally 6 years. If you have information that is beyond this period you inadvertently add time to a request as you have more documents to go through. Practicing data hygiene by deleting old documents when the retention period is over would reduce the time spent on searching documents.

Please note that having more data whether on the server or an external disk drive would not trigger an extension.

- Needing to obtain specialist legal advice. If you routinely obtain legal advice (for example, where lawyers are responsible for responding to, or reviewing DSARs), it is unlikely to be complex.
- Searching large volumes of unstructured manual records (only applicable to public authorities).

Requests that involve a large volume of information may add to the complexity of a request. However, a request is not complex solely because the individual requests a large amount of information.

How to Calculate the DSAR Timeline

A calendar month starts on the day the organisation receives the request, even if that day is a weekend or public holiday. It ends on the corresponding calendar date of the next month. Remember to stop the clock whilst awaiting identity verification and/or clarifying information and restart the clock on the receipt of these.

> Example
> An organisation receives a request on 3 September. The time line starts on 3 September, giving the organisation until 3 October to comply with the request. If the end date falls on a weekend or a public holiday, the deadline is extended to the next working day.
> From the Information Commissioners Office

> Example
> An organisation receives a request on 25 November. The time line starts from the same day. The corresponding calendar date is 25 December, but 25 December and 26 December are bank holidays. So the organisation would therefore have until the next working day, 27 December if that was a week day.
> From the Information Commissioners Office

> Example
> If you receive a request on 14 May, the time limit starts from the same day. You will have one month to reply which means you should respond by or on 14 June. However, if you ask for clarification on 15 May, the clock stops from 15 May until the date the requester responds. If the requester provides you with clarification on 18 May, the timing will resume on that date.
> The clock was therefore stopped from 15 May until 18 May. This means that you can extend the original one month deadline by three days and you should provide a response by or on 17 June.
> From the Information Commissioners Office

You can extend the response time by a further two months if the request is complex (as detailed in the section on The Two Month Extension) or you have received a number of requests from the individual – this can include other types of requests relating to individuals' rights. For example, if an individual has made a DSAR, a request for erasure and a request for data portability simultaneously.

You should calculate the extension as three months from the original start date, i.e. the day you receive the request or other requested information.

Can we charge a fee?

The GDPR states that you can no longer charge a fee for responding to a subject access request. However, you can charge a 'reasonable fee' for the administrative costs of complying with a request if:

- it is manifestly unfounded or excessive; or
- an individual requests further copies of their data following a request.

A request may be manifestly unfounded if for example, 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.

You must consider a request in the context in which it is made. If the individual genuinely wants to exercise their rights, it is unlikely that the request is manifestly unfounded.

Example
An individual makes a subject access request to an online retail company for their personal data. They state that they are making a DSAR in accordance with the UK GDPR and that if the company credits the individual's online account with a specified sum of money, they will withdraw their request. The company is correct to consider the request as manifestly unfounded.

From the Information Commissioners Office

If you refuse to comply with a request, you must inform the individual of:

- the reasons why;
- their right to make a complaint to the ICO; and
- their ability to seek to enforce this right through the courts

If you believe a request is manifestly unfounded or excessive, you must be able to demonstrate this to the individual.

A growing awareness of data protection rules has contributed to an increase in people filing subject access requests. For companies or organisations that do not have a clear process in place, handling these requests can be particularly challenging. Following the guidance in this document will give you a good place to start, but does not constitute legal advice. Specialist data protection lawyers can assist you further, whether you are looking for light touch advice or for someone to manage the process of handling a DSAR on your behalf.

Checklist

Preparing for Data Subject Access Requests

- ☐ We know how to recognise a subject access request and we understand when the right of access applies.
- ☐ We have a policy for how to record requests we receive verbally.
- ☐ We understand what steps we need to take to verify the identity of the requester, if necessary.
- ☐ We understand when we can pause the time limit for responding if we need to ask for clarification.
- ☐ We understand when we can refuse a request and are aware of the information we need to provide to individuals when we do so.
- ☐ We have suitable information management systems in place to allow us to locate and retrieve information efficiently.

Complying with Data Subject Access Requests

- ☐ We have processes in place to ensure that we respond to a subject access request without undue delay and within one month of receipt.
- ☐ We understand how to perform a reasonable search for the information.
- ☐ We understand what we need to consider if a third party makes a request on behalf of an individual.
- ☐ We are aware of the circumstances in which we can extend the time limit to respond to a request.
- ☐ We understand how to assess whether a child is mature enough to understand their rights.
- ☐ We understand that there is a particular emphasis on using clear and plain language if we are disclosing information to a child.
- ☐ We understand what we need to consider if a request includes information about others.
- ☐ We are able to deliver the information securely to an individual, and in the correct format.

Westbrook
Data Protection Services

Get in touch

wdps.co.uk

E: info@wdps.co.uk

T: 079 7693 9016

Westbrook Data Protection Services is a limited company registered in England and Wales with registered number 09518843. The registered office is 2nd Floor, Midas House, 62 Goldsworth Road, Woking, GU21 6LQ