

GDPR – Subject Access Request Policy

1. Introduction

Article 15 of the General Data Protection Regulations (GDPR) provides individuals (Data Subjects) with the right to access personal information so that they are fully informed of the nature of any processing and to verify the lawfulness of Doc Abode Ltd's processing of their personal data.

The right allows them to obtain confirmation as to whether personal data is being processed by Doc Abode Ltd, and where it is being processed, they are entitled to access the following information:

- A copy of the data (subject to any exemptions)
- The reasons why their data is being processed.
- The description of the personal data concerning them.
- Anyone who has received or will receive their personal data.
- Details of the origin of their data if it was not collected from them.

This right of access extends to all information held about the Data Subject, for example registration details, activity details and emails that refer to them.

Data Subjects requesting their information must submit a Subject Access Request (SAR) to Doc Abode Ltd which outlines what information they wish to receive and proof of their entitlement to access it (Proof of identity).

Under the General Data Protection Regulations, some personal data is exempt from disclosure if disclosing it would 'adversely affect the rights and freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software.' The UK Data Protection Act 2018 introduces further exemptions to SARs such as those for national security, defence, law enforcement and public security.

The Policy sets out the manner by which Doc Abode Ltd will respond to Subject Access Requests.

2. Purpose

This policy standardises how Doc Abode Ltd will manage SAR's so as to ensure that:

- Data Subjects are provided with a clear, efficient and easy to use means of requesting access to their personal information.
- SAR's received by Doc Abode Ltd are recognised, logged and acknowledged in a timely manner.
- The location and retrieval of personal data within the scope of a SAR is efficient and thorough.
- Staff asked to provide information in response to a SAR are aware of their duties and responsibilities to comply with the requests.
- Responses to SARs are consistent and fully deliver against the rights of the individuals.
- Any exemptions to the rights to access are applied appropriately and documented accordingly.

3. Scope

This policy and associated procedures applies to:

- All staff, contractors, consultants, student workers, temporary workers, shared services, and data processors who have access to Doc Abode Ltd systems or data.
- All Data Subjects about whom Doc Abode Ltd processes personal data.
- Data held on all Doc Abode Ltd information and systems, whether hosted on site or in the cloud, on portable storage media or devices or paper.

4. Responsibilities

The Information Governance Officer will be the individual with operational responsibility for processing Subject Access Request in line with the requirements of the GDPR.

All staff are responsible for ensuring that they recognise a Subject Access Request and to forward it, or direct the requestor onto the Information Governance Officer immediately. All staff who are requested by the Information Governance Officer to conduct a search for information and to provide it in response to a SAR, must do so as soon as they are contacted.

5. Receiving Requests

A SAR can be made in a number of different ways, including via telephone or in person, but for it to be considered a valid request, it must be clear what the data subject is requesting, they must provide proof of their identity so as to verify their right to access the data.

Doc Abode Ltd will always encourage the requestor to submit the request in writing so as to provide a clear audit trail of the request and to ensure that both the requestor and Doc Abode Ltd have a clear record of what was requested. If the requester advises that a written request is not possible, the Doc Abode Ltd Information Governance Officer will liaise with them to facilitate an alternative method of submission.

Written requests may be received via letter or email.

Where a request is considered too vague to be processed, the requestor shall be contacted to provide clarity. The request may not be considered valid until it is clear precisely what information is being requested.

Requests made by third parties acting on behalf of a data subject will be accepted, but they must be accompanied a copy of written authority from the Data Subject or written authority such as Power of Attorney (if applicable) and proof of the Data Subjects identity. Requestors who cannot provide this will be refused until such time that they can.

Acceptable proof of identity shall be any of:

- A copy of Photographic ID such as passport, driving licence or Student ID (originals are not required, but can be copied if presented in person)
- Birth Certificate
- Two utility bills or bank statements (with redacted transactions) containing a full address of less than 3 months old.

Requests made by third parties who are not acting on behalf of a data subject will be accepted, but they must be accompanied a letter showing their written authority to make such requests, for example Police and law enforcement agencies must state the exemption to the right to access under the Data Protection Act 2018 that they believe entitles them to access information.

The Information Governance Officer shall consider the validity of any request of this nature in consultation with the Data Protection Officer. Doc Abode Ltd will refuse any requests that it considers does not engage the exemption stated in the request.

6. Fees

There is normally no charge for receiving a copy of information requested through a SAR, however a 'reasonable fee' may be applied when a request is deemed to be manifestly unfounded, excessive or repetitive.

Any “reasonable fee” will be calculated based on the administrative cost of providing the information. Doc Abode Ltd will notify the requestor of any reasonable fee within a month of the receipt of the original request, along with an explanation as to why the fee is applied.

7. Timescales

The time period to respond to a SAR begins upon receipt of a valid request. If a request is sent to an account responding with an automatic ‘out of office message’ that contains a valid alternative contact, the person submitting the request is responsible for re-sending the request to the alternate email address. Failure to send the email to the alternate email address will mean that the request will not be considered to have been “received”.

Responses to SARs will be provide without delay and at the latest within one month of their receipt.

8. Locating Requested Information

Once a valid request has been received, the Information Governance Officer will establish the nature and likely location of the information the requester has asked for. He/she will contact the relevant system, process, or account owners that have been identified as likely to hold this information and will explain what information is required and alert the relevant people on the deadlines that need to be met - usually no later than 10 working days before the deadline for disclosure.

9. Screening Information

Once all information believed to be within the scope of the request has been returned to the Information Governance Officer, it will then screened and reviewed for the presence of any third party data that the data subject is not entitled to receive. This may result in the removal or redaction of such information unless the third party has consented to disclosure; or it is reasonable in all circumstances to comply with the request without seeking the third party individuals consent.

10. Providing Information

Following screening, the Information Governance Officer will collate the formal response to the request including a copy of the data and an explanation of any exemptions that have been applied, plus either a copy of the relevant Privacy Notice or any required additional description of:

- The personal data concerning them.
- The reasons why their data is being processed.
- Details of anyone who has received or will receive their personal data.
- Details of the origin of their data if it was not collected from them.

The format of the disclosure will be made in line with the requestor’s preference whenever possible. Where the requestor has not specified a preferred format, Doc Abode Ltd will provide the information using an appropriately secure electronic transfer method such as the corporate Office356 system.

The communication will set out the requestors subsequent rights to:

- Request another search if they have believe information is missing.
- Request that inaccurate information be rectified or erased.
- The existence of any right to object to or restrict processing
- Their right to complain to the ICO if they are unhappy with the disclosure.

11. Data Processors and Subject Access Requests

When procuring a service provider to undertake work on behalf of Doc Abode Ltd, appropriate protocols will be agreed to ensure that data processors are aware of their responsibility to

assist with subject access requests and to provide information (where necessary) that they may hold relevant to a subject access request received by Doc Abode Ltd.

12. Monitoring of SAR responses

The Information Governance Officer shall regularly review the handling of and responses to SARs, to ensure ongoing compliance, identify issues and ensure the quality and consistency of responses.

13. Policy Review

This policy will be reviewed on an annual basis or sooner as is required e.g. where there are changes in legislation, or recommended changes to improve best practice.