

RRL LLP

Subject Access Request (SAR)

Purpose

The General Data Protection Regulations 2018 (GDPR) gives individuals (data subjects) rights, including the right to access personal data that an organisation holds about them. When an individual makes a request to view their information it is known as a 'subject access request'. This document sets out our policy for responding to an individual's subject access request under GDPR.

Policy

RRL LLP (LLP) is committed to operating openly, transparently, and to meeting all reasonable lawful requests for information that are not subject to specific exemption in the Act.

Subject Access Request Procedure

Right of Access

Making a Subject Access Request (SAR)

In the first instance all applicants should contact us via email at michelle.pearce@rrlcornwall.co.uk or by calling 01872 276116.

The following requirements must be met for a SAR to be valid:

- a) The applicant must submit a written Subject Access Request.
- b) The applicant must supply two forms of identification: (1) Identification with a photograph and signature e.g. passport, and (2) Identification with proof of name and address e.g. a recent bank statement or utility bill (issued in the last three months)
- c) The applicant must supply any further information that is reasonably required to assist us in locating information relevant to the request.

How we process Subject Access Requests:

- a) We will first check that we have enough information to confirm your identity. If we have any cause to doubt your identity we will ask you to provide any evidence we reasonable need to confirm your identity.
- b) We will check that we have enough information to find the information you requested. If we need more information from you to assist us in our search we will promptly request this from you.
- c) We will identify if any of the information gathered was provided by or identifies a third party.

If we identify information that relates to third parties we will take all reasonable steps to establish whether this information can be disclosed. We are not required to disclose information relating to third parties, unless they have provided their consent or it is reasonable to do so without their consent. If the third party objects to the information being disclosed we may seek legal advice on what action we should take. Before sharing any information that relates to third parties, we will where possible anonymise information that identifies individuals not already known to the applicant. We will also edit information that may affect another party's privacy, and if necessary summarise the information provided (rather than provide a full copy of the document).

- d) Once we have confirmed identification, resolved any queries around the applicant's request, and gathered the relevant information, we will issue our response electronically via a secure email service, or if requested, via hard copy. Hard copy responses will be sent by Royal Mail recorded delivery in an envelope or package marked 'Private and Confidential' and 'Addressee Only'.

The cost of a Subject Access Request

We do not routinely charge a fee for Subject Access Requests. However, if you have requested a hard copy response then we reserve the right to charge the actual costs of sending the response by Royal Mail recorded delivery. If you do not want to pay this, when requested, you may choose to receive your response electronically at no charge. If you have any questions regarding the costs for receiving a hard copy response then please contact us on the details outlined in 1.1.

Timeframe for responding to Subject Access Requests

The General Data Protection Regulation requires that a full response must be sent within one calendar month starting from the date when we received all the information necessary to identify you and identify the information requested. We will aim to respond to all requests as soon as possible within this timeframe.

Grounds for not complying with Subject Access Requests

The General Data Protection Regulation contains a number of exemptions to our duty to disclose personal data, and we may seek legal advice if we believe one or more of these exemptions may apply to the request. Details of these exemptions can be found on the Information Commissioner's Office (ICO) [website](#).

If you have made a previous subject access we must respond only if a reasonable interval has elapsed since this previous request was made. We will define a reasonable interval by reviewing the elapsed time, nature of information, and changes that have occurred since the last request was made.

Right to Rectification

What to do if you identify inaccurate information in our records

If you identify an error in the information we hold please notify us as soon as possible. If we agree that the information is inaccurate we will take all reasonable steps to correct the information or if relevant and practically possible, remove the inaccurate information by deletion or destruction. If we believe the information is accurate, or we are unable to make a decision as to the accuracy of the information, we will keep a note of the alleged error on the file.

Right to Erasure (Right to be Forgotten)

The Right to Erasure applies in the following circumstances:

- The personal data is no longer necessary in relation to the purpose for which it was originally collected
- The processing was based on consent, and the Data Subject has now withdrawn their consent
- The Data Subject objects to processing and there is no overriding legitimate interest of the Data Controller
- The data was being unlawfully processed
- The data must be erased to comply with a legal obligation

Right to Restrict Processing

What to do if you want us to stop processing your data.

Under Article 17 of the GDPR individuals have the right to have personal data erased. This is also known as the 'right to be forgotten'. The right is not absolute and only applies in certain circumstances. The right to prevent processing applies in certain limited circumstances, and specific processes must be followed to make the objection. Further details can be found on the Information Commissioner's Office (ICO) [website](#). We will respond to an objection (section 10) notice within 21 days of receipt, and in writing, advising that we have either complied with your request, intend to comply with it, or state the extent to which we will comply with it and why.

Right to Data Portability

This Right allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows the individual to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way in a common data format, for example, Excel or CSV file.

The Right to Data Portability applies in the following circumstances:

- When the personal data was provided to the controller directly by the Data Subject
- Where the processing is based on consent or performance of a contract
- When processing is carried out by automated means.

Right to Object

An individual has the Right to Object to:

- Processing based on legitimate interest or performance of a task in the public interest/exercise of official authority (including profiling)
- Direct marketing (including profiling)
- Processing for the purposes of scientific/historical research and statistics.

Rights in Relation to Automated Decision Making and Profiling

This Right provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention.

The Right not to be subject to a decision applies when:

- It is based on automated processing
- It produces legal/significant effects on the individual

It does not apply if the decision:

- Is necessary for entering into or performance of a contract
- Is authorised by law
- Is based on explicit consent
- Does not have a legal/significant effect on the data subject

Our complaints procedure

An individual having any complaint in connection with our actions has the right to present a complaint in writing to a Partner of RRL LLP.

If you remain dissatisfied, you have the right to report your concern to the Information Commissioner's Office (ICO).