



Cambridge • 01223 209888
Chelmsford • 01245 708808
Ipswich • 01473 250990
Norwich • 01603 216450

Subject Access Request (SAR) Policy

Purpose

This policy explains how Pure Resourcing Solutions Limited handles Subject Access Requests (SARs) under the UK GDPR and Data Protection Act 2018.

It sets out how requests are recognised, logged, assessed, searched, responded to and escalated. The right of access allows individuals to obtain confirmation that their personal data is being processed, a copy of that data and supplementary information about how it is processed.

Scope

This policy applies to all employees, workers, contractors and anyone who receives or handles a Subject Access Request.

It applies to personal data held in electronic systems, paper files, emails, shared drives, recruitment systems, archived records and any other relevant record format.

It covers requests relating to candidates, employees, clients, suppliers and all other individuals whose personal data is processed by the organisation.

Recognising a Subject Access Request

A Subject Access Request may be made verbally or in writing, including by:

- email;
- letter;
- telephone;
- social media;
- in person; or
- through any other communication channel.

The requester does not need to mention "Subject Access Request", "SAR" or UK GDPR for the request to be valid.

Any employee who receives a request must:

- record the date it was received;
- forward it to the Data Protection Lead within one working day; and
- not attempt to answer the request themselves.

What an Individual Can Request

An individual is entitled to:

- confirmation that their personal data is being processed;
- a copy of their personal data; and
- supplementary information required by Article 15 UK GDPR.



Cambridge • 01223 209888
Chelmsford • 01245 708808
Ipswich • 01473 250990
Norwich • 01603 216450

This supplementary information includes:

- purposes of processing;
- categories of personal data;
- recipients or categories of recipients;
- retention periods;
- source of the data where it was not collected directly from the individual;
- information about automated decision-making where applicable;
- details of the individual's rights;
- the right to complain to the Information Commissioner's Office.

Responses should be provided in plain language and explain any technical terminology, abbreviations or recruitment-specific codes where necessary.

Definitions

Data Controller

The organisation that determines why and how personal data is processed.

Personal Data

Any information relating to an identified or identifiable living individual.

Special Category Data

Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health information or data concerning a person's sex life or sexual orientation.

Identity Verification

Identity verification should only be requested where there are reasonable doubts about the identity of the requester.

Any evidence requested must be proportionate and limited to what is necessary.

Where someone is acting on another person's behalf, the organisation should obtain appropriate evidence of authority, such as written consent, parental responsibility or a valid power of attorney.

Searching for Personal Data

The organisation will conduct reasonable and proportionate searches across all systems likely to contain the individual's personal data.

Depending on the circumstances, this may include:

- recruitment CRM and candidate database;
- email accounts and archived mailboxes;
- interview notes;
- CVs and candidate records;
- client records;
- compliance documentation;
- shared drives;



Cambridge • 01223 209888
Chelmsford • 01245 708808
Ipswich • 01473 250990
Norwich • 01603 216450

- HR files;
- paper records;
- call recordings (where retained);
- marketing databases.

Managers should provide requested information promptly, normally within five working days of receiving the request from the Data Protection Lead.

Searches should be sufficiently comprehensive to identify personal data held at the time the response is prepared.

Where clarification is genuinely required to identify the requested information, the organisation may ask the requester to clarify the scope of the request.

Third-Party Information

Before disclosing information, the organisation must review documents for personal data relating to other individuals.

Where possible, third-party information should be:

- redacted;
- anonymised; or
- separated from the disclosure.

Where this is not possible, the organisation will balance the requester's right of access against the rights and freedoms of the third party before deciding whether disclosure is appropriate.

Exemptions

Not all information must be disclosed.

The organisation may rely upon exemptions provided by the Data Protection Act 2018, including where information is protected by:

- legal professional privilege;
- management forecasting or planning;
- confidential references (where applicable);
- crime and taxation exemptions;
- negotiations with the requester;
- protection of the rights and freedoms of others.

Each exemption will be considered individually and documented.

Response Format

Information will normally be provided electronically in a commonly used format unless the requester asks otherwise or this would be unreasonable.



Cambridge • 01223 209888
Chelmsford • 01245 708808
Ipswich • 01473 250990
Norwich • 01603 216450

Where appropriate, information may be disclosed securely through encrypted email or another secure transfer method.

Responses should be:

- concise;
- transparent;
- intelligible; and
- easy to understand.

Time Limits

The organisation will respond without undue delay and within one month of receiving the request. Where identity verification is reasonably required, the one-month period begins once sufficient information has been received to verify the individual's identity.

The deadline may be extended by up to two further months where requests are complex or numerous. Where an extension applies, the individual will be informed within the initial one-month period together with the reasons for the extension.

Manifestly Unfounded or Excessive Requests

The organisation will not normally charge a fee.

A reasonable fee may only be charged where a request is manifestly unfounded or excessive. Alternatively, the organisation may refuse to act on such a request where permitted by law.

Any such decision must be documented and approved by the Data Protection Lead.

Refusals and Partial Refusals

Where the organisation refuses all or part of a request, it will notify the individual without undue delay and within one month.

The response will explain:

- the reasons for the refusal;
- any exemptions relied upon;
- what information has been withheld (where appropriate);
- the right to complain to the Information Commissioner's Office;
- the right to seek a judicial remedy.

Accuracy Concerns

If information identified during a Subject Access Request appears to be inaccurate, the organisation should consider whether correction is appropriate.

The right to rectification is separate from the right of access.



Cambridge • 01223 209888
Chelmsford • 01245 708808
Ipswich • 01473 250990
Norwich • 01603 216450

Where the organisation does not agree that correction is required, it will record the individual's objection or note of dispute where appropriate.

Record Keeping

All Subject Access Requests must be logged centrally.

Records should include:

- date received;
- requester details;
- identity verification undertaken;
- scope of the request;
- systems searched;
- departments involved;
- exemptions considered;
- decisions made;
- response date;
- any extensions;
- any refusals or partial refusals;
- fees charged (if applicable).

The organisation will maintain an audit trail demonstrating compliance with UK GDPR.

Responsibilities

Data Protection Lead

Responsible for:

- overseeing Subject Access Requests;
- monitoring statutory deadlines;
- coordinating searches;
- approving refusals;
- maintaining records;
- ensuring legal compliance.

IT Function

Responsible for:

- assisting with system searches;
- retrieving archived information where appropriate;
- exporting electronic records securely;
- supporting secure disclosure.

Managers

Managers must ensure their teams respond promptly to search requests and provide relevant information within required timescales.



Cambridge • 01223 209888
Chelmsford • 01245 708808
Ipswich • 01473 250990
Norwich • 01603 216450

Employees

Employees must recognise Subject Access Requests, forward them immediately to the Data Protection Lead and cooperate fully with any internal searches.

Contact Details

Subject Access Requests should be sent to:

Email: privacy@prsg.co.uk

Telephone: 01223 209888

Post:

Pure Resourcing Solutions, The Workspace, Pioneer Court, Vision Park, Histon, Cambridge, CB24 9PT

Individuals who remain dissatisfied may complain to the Information Commissioner's Office (ICO) or, where applicable, another relevant supervisory authority if their personal data is processed outside the UK.

Policy Ownership

Responsible: Quality, Compliance Systems Team Leader

Accountable: Operations Director

Consulted: Management Team

Informed: All employees, candidates and contacts

Policy Review

This policy will be reviewed annually, or sooner where changes to legislation, ICO guidance or organisational processing activities make this necessary.