# Data Subject Rights & Subject Access Request Procedure

Mogas Design Ltd | Version 1.0 | Issued: 18 October 2026

## 1. Purpose and scope

This procedure explains how Mogas Design Ltd recognises, records, considers and responds to requests made by individuals about their personal data in accordance with UK GDPR, Data Protection Act 2018 and relevant Data (Use and Access) Act 2025 amendments. It applies to both directors and independent contractors handling information on behalf of Mogas. It does not imply Mogas has employees.

## 2. Responsibility and reporting route

A designated director acts as Data Rights Lead and is responsible for the request log, deadlines, identity checks, scope, searches, exemptions, response approval and record retention. All directors and contractors must forward any apparent rights request promptly to the director through the normal company contact email. People need not use a particular form, terminology or channel: verbal and written requests can be valid. Where Mogas acts only as a processor for a client, promptly notify that client and assist under the applicable agreement; do not respond independently unless authorised.

## 3. Rights covered

The procedure covers access (SAR), rectification, erasure, restriction, objection, portability (where applicable), and rights relating to solely automated decision-making where relevant. Each right has legal conditions and possible exemptions; a request is not automatically an entitlement to every action sought.

## 4. Receipt, logging and acknowledgement

Record date/time and method received, requester, right invoked, systems potentially involved, owner, statutory due date, identity/authority status, clarification and any paused period, decision, communications, secure disclosure method and closure. Send a prompt acknowledgement where practical. Record verbal requests in writing. The optional Mogas Subject Access Request Form may help, but completion is never mandatory.

## 5. Verify identity and representative authority

Use proportionate checks only where reasonable doubts exist, taking into account the sensitivity and risk of disclosure. Avoid routine requests for passports or excessive identification; verify using an established contact route when possible. For requests via an agent, verify appropriate authority. Request necessary evidence promptly and store it securely for no longer than needed. Where the law permits, the response clock begins once reasonably required identity or authority information is received.

## 6. Response times and extensions

Respond without undue delay and normally within one calendar month. Calculate deadlines from the applicable start date; do not assume 30 days. For complex requests or several requests from the same individual, an extension of up to two further months may be allowed; notify the person of the extension and reasons within the original period. For a SAR, clarification can pause the clock only where genuinely and reasonably required to respond; document why and record the pause/resumption. Do not insist that a requester narrow their request.

## 7. SAR search, review and disclosure

Carry out reasonable and proportionate searches of relevant email, cloud project folders, finance/contact systems, contractor-held information and any other relevant locations. Search for the requester's personal data (not indiscriminately every document containing a name). Identify third-party data, confidential material, legally privileged information and applicable statutory exemptions before disclosure. Redact third-party material where appropriate and give supplementary information required by Article 15. Communicate securely in a commonly used accessible format, after verifying the intended recipient.

## 8. Erasure and other rights

For deletion requests identify the information, purpose, lawful basis and any need to retain it (including relevant tax, contractual or legal-claims obligations). Delete only where the right applies and no exception prevents it; otherwise explain the decision, including partial deletions. Consider notifying relevant recipients where required. For rectification, correct verified errors and consider disputed-data annotations. For restriction, objection or portability, assess the legal criteria and take and document appropriate action. Where data is held for a client as controller, coordinate with the client.

## 9. Charges, refusals and complaints

Rights requests are generally free. A reasonable charge or refusal may be permissible in limited cases, for example manifestly unfounded or excessive requests; record the evidence and reasoning and obtain director approval. Give a clear explanation, the right to complain to the Information Commissioner's Office (ICO), and available routes to seek a judicial remedy as required by law. Requests and complaints must not cause retaliation.

## 10. Secure handling and data minimisation

Restrict the request log and evidence to authorised persons; use company-controlled systems, suitable access controls and secure transfer methods. Do not send client drawings, personal financial records or other people's information without review. Any misdirected response or suspected personal-data breach must be escalated immediately and assessed under the company Information Security Policy and breach-response arrangements.

## 11. Records and review

Retain a proportionate audit trail of requests, searches, decisions, disclosures, exemptions and review actions for a documented period aligned with the company retention schedule. Review this procedure at least annually and after material legislative, processing or contractual changes. Brief relevant contractors on how to recognise and escalate requests. Refer to the Mogas ROPA, Information Security Policy and SAR Form.

## Operational checklist

- Recognise and log the request, allocate a director, and set the deadline.
- Verify identity/representative authority only when needed; promptly document any clarification.
- Search proportionately; review exemptions and third-party information.
- Approve the decision and respond securely within the correct deadline.
- Document closure, evidence retained and lessons learned.

## Document control & director approval

| | |
|---|---|
| **Document number** | **MOG-DP-PRO-002** |
| **Revision** | 1.0 |
| **Prepared / review date** | 18 October 2026 |
| **Next planned review** | 18 October 2027 |
| **Approving director** | Mohammed Fasiuddin |
| **Status** | Approved by the Director |

Director signature:

Signed copy held on file – available on request.

Reference guidance: ICO – A guide to subject access; Right to erasure; Data Use and Access Act 2025 overview (accessed October 2026).