# Personal Data Breach Notification Procedure

**UK GDPR • Data Protection Act 2018 • Revision 0 • 18 October 2026**

## 1. Purpose and scope

This procedure explains how Mogas Design Ltd identifies, contains, investigates, records and, where required, reports personal data breaches. It applies to both directors and all independent contractors with access to Mogas systems, project material or personal data, whether working remotely, from a home office or during gas-site visits. A personal data breach includes accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

## 2. Responsibilities and reporting route

The nominated director, Mohammed Fasiuddin, coordinates incident response, assesses legal notification duties, liaises with clients, processors and the ICO, and approves case closure. Any director or contractor who suspects a breach must contact the nominated director immediately using the company's established direct contact route; do not wait to establish whether the incident is reportable. Contractors must preserve evidence, follow instructions and promptly identify affected client systems or third parties. The director will appoint an alternative decision-maker if personally unavailable or implicated.

## 3. Examples of incidents

Misaddressed emails; lost or stolen laptops/phones; files sent to the wrong client; unauthorised cloud sharing links; compromised logins; malware/ransomware; loss of records; accidental deletion without recoverable copies; and unauthorised access to contact lists, supplier bank details, ID records or site-visitor information. Engineering drawings without personal data may represent an information security incident rather than a personal data breach; assess their contents before classifying.

## 4. Immediate response and containment

Protect individuals and evidence first. Where safe, stop further disclosure; revoke shared links, disable compromised accounts, reset credentials, isolate affected devices and contact the IT/cloud provider if necessary. Do not delete logs or destroy evidence. Record when the incident was discovered, when Mogas became aware of a personal data breach, what data may be affected, who may be affected and what containment actions have been taken. Escalate concurrent safety or operational risks through client/site emergency procedures.

## 5. Assess impact and reporting thresholds

Assess the likelihood and seriousness of harm to individuals: data sensitivity, volume, identifiers, financial details, ability to identify people, extent of disclosure, encryption/access protections and potential for identity fraud, distress or discrimination. Where Mogas is the controller, notify the ICO unless the breach is unlikely to result in a risk to people's rights and freedoms. Where high risk is likely, also inform affected individuals without undue delay, unless a lawful exception applies. Record reasons for reporting or not reporting; every confirmed personal data breach must be documented, even when notification is unnecessary.

## 6. Notification timetable and content

A reportable breach must be notified to the ICO without undue delay and, where feasible, within 72 hours after Mogas becomes aware of it—not 72 hours after the investigation finishes. If information is incomplete, submit what is known and update later; explain any delay beyond 72 hours. The director records the notification deadline, submission reference and subsequent updates. Notification should identify breach nature, approximate numbers and categories of people and records, contact point, likely consequences and remedial measures. Individuals facing high risk must be told promptly in clear language, with practical protective advice.

## 7. Controller, processor and client relationships

Determine whether Mogas acts as controller or processor for the relevant data. If Mogas acts as a processor, notify the relevant controller without undue delay under contractual and UK GDPR obligations, and cooperate with its investigation; do not assume that reporting directly to the ICO replaces notification to the controller. Where a cloud provider or other processor has an incident affecting Mogas-controlled data, require prompt notice and enough information to assess risk. Follow contractual client notification requirements, including any shorter deadlines.

## 8. Investigation, corrective actions and close-out

The director documents timeline, root cause, affected systems, harm assessment, notifications and evidence; assigns corrective actions with owners and dates; checks effectiveness before closure; and assesses whether passwords, permissions, training, supplier contracts, retention practices, backups or other controls need change. Preserve records securely and limit access to authorised persons. Update the risk register and related policies where lessons learned justify changes.

## 9. Confidential register and retention

Maintain an internal Personal Data Breach Register containing incident ID; discovery and awareness times; reporter; breach description; data categories and estimated affected individuals/records; controller/processor role; containment; risk rating; ICO notification decision, deadline and reference; individuals/client notification; decisions/exemptions; corrective action owner; closure date; and evidence link. Retain records in restricted company cloud storage under a documented retention schedule; avoid keeping unnecessary copies of compromised personal data.

## 10. Review and awareness

Directors review this procedure at least annually, after a material breach or following relevant legal or systems changes. Communicate the reporting route and duties to each relevant contractor at onboarding and retain acknowledgement evidence. Test response readiness proportionately, for example with a brief tabletop scenario.

## First-response checklist

- Report immediately to the nominated director; log discovery and awareness times.
- Contain the exposure and preserve logs, emails, screenshots and relevant evidence.
- Confirm what personal data and whose information may be involved.
- Establish Mogas controller/processor status and client/contractual notification duties.
- Assess risk to individuals; set ICO 72-hour deadline if potentially reportable.
- Determine whether affected individuals must be notified without undue delay.
- Record outcome, corrective actions, review and closure.

## Document control and director approval

| | |
|---|---|
| Document number | MOG-DP-PDB-001 |
| Revision / prepared | 0 / 18 October 2026 |
| Review due | 18 October 2027, or earlier if required |
| Document owner | Mohammed Fasiuddin, Director |
| Approval status | Approved by the Director |

Director signature:

Signed copy held on file – available on request.

Reference: ICO, “Personal data breaches: a guide” (accessed 18 October 2026). This procedure does not assert ICO notification is required for every incident.