GDPR staff reporting and handling instructions

AIVS Software Limited | All employees directors contractors and temporary staff

Protect personal information in all forms, including email, documents, software, paper and AI outputs. These instructions explain immediate staff reporting and the records used by assigned case handlers. Read them with the current AIVS privacy notices, approved procedures and the software HELP guides.

1 Report promptly and use the correct route

Report to the Designated Director responsible for data protection, using the current reporting contact details issued by AIVS. Report suspected breaches, information requests, privacy complaints and proposed changes involving personal information promptly. For a suspected breach, report immediately, even if the facts are incomplete.

For an urgent incident, make direct contact as well as sending an email record. If the Designated Director is unavailable, unreachable or involved, or you do not have the current contact details, contact another AIVS Director immediately. Do not wait for an email reply, a completed form, software access or proof of harm.

All staff must report and preserve facts. The Designated Director or alternate assigns the handler and IT support. Only assigned, authorised staff should investigate, access a case or communicate a response. The application records handler and approver details but does not restrict cases to that handler or route approval requests. Obtain actual approval outside the application before recording it. A software record or the software feedback link does not replace urgent reporting.

2 Recognise and protect personal information

Personal information identifies someone directly or indirectly: names, work email addresses, staff and client records, account identifiers, images, messages and identifiable activity logs. Health information, biometrics used to identify someone and other special-category information need additional protection. A reference number or removal of a name does not necessarily make a record anonymous. [1]

Use information fairly and only for an approved, lawful purpose. Tell people how it is used through the appropriate privacy notice. Collect and share only what is necessary, keep it accurate, keep it only as long as needed, secure it and retain evidence of the actions taken. Do not invent a new purpose, lawful basis or consent process yourself. [1]

Use approved systems and your own account; protect passwords, email codes and authenticator codes. Check recipients and sharing permissions before sending. Keep screens, devices and paper secure. Avoid unnecessary exports or copies in personal email, private storage or unapproved messaging tools. Report a mistake immediately instead of trying to conceal it.

3 Use the GDPR application

Open the approved GDPR application: https://agivs.co.uk

Sign in with your own authorised AIVS email address, the email verification code and your phone-authenticator code. Follow the first-use authenticator setup when prompted. Access to a menu does not authorise you to browse other people's cases. Open or change only records needed for work assigned to you.

Menu	Use
G1 Staff	Staff or applicant personal-information requests and privacy complaints.
G2 Clients	Client personal-information requests and privacy complaints.
G3 CYBER(login)	Opens CYBER in a separate tab, with its own sign-in.
G4 Audit trail	Read-only saved activity and backup status; not proof that a response was delivered.

© 2026 AIVS. All rights reserved.

Menu	Use
G5 Data breaches	Incident records and preparation of ICO notification drafts.

Use HELP beside each case section for its detailed instructions. HELP opens a separate PDF tab; close that tab to return to the application. If the screen differs or access fails, contact the Designated Director or the application administrator and continue urgent reporting by the direct route above.

Save explicitly and wait for confirmation before leaving. G1 and G2 use Save case; G5 uses Save breach record. A draft or an open HELP page is not a saved record. Unsaved work can be lost on reload or sign-out. If a connection fails, keep the tab open and check the saved record before retrying; the server may have saved it. Follow the different conflict instructions for G1/G2 in section 5 and G5 in section 6.

4 Receive a request or privacy complaint

A person may ask verbally or in writing for access, correction, deletion, restriction or other rights, or complain about how information was used. No special form or legal wording is necessary. Preserve the original words, receipt date and time, contact method and any requested outcome; send them promptly to the Designated Director. Do not refuse a request, promise deletion or disclose information yourself. [2-3]

A subject access request normally requires a response without undue delay and within one calendar month, subject to the applicable legal timing rules. A privacy complaint must be acknowledged within 30 days, investigated and answered without undue delay. The complaint acknowledgement period is not a 30-day deadline for answering every rights request. Where both apply, the handler must track both duties. [2-3]

The lead checks identity and authority proportionately, sets the deadline and records the reason for any lawful pause or extension. Staff must not reset the original receipt date, assume that a status change pauses time, or ask for excessive identity documents. Preserve relevant records and cooperate with the authorised search. Do not alter or delete information to frustrate a request.

5 Record and manage requests in G1 or G2

Assigned case handlers use G1 Staff → Add staff case or G2 Clients → Add client case. Choose Personal information request or Privacy complaint. Use the five numbered software sections below. Keep full correspondence and identity evidence in the approved restricted case folder; enter minimum necessary details and evidence references in the register.

1 Intake and responsibility

Record the person or reference, company and known contact details, Original receipt date, Case handler, summary and scope. Record AIVS's controller or processor role, rights requested and Restricted case folder reference. Use Save case and wait for confirmation and a permanent GDPR-S- or GDPR-C- reference.

2 Timing and identity checks

Record the acknowledgement, proportionate identity or authority checks, Deadline basis, original and current due dates and reasons for changes. G1 and G2 do not calculate legal deadlines. The lead must check the dates; an Awaiting information or Extended status does not itself change the law.

3 Actions and evidence

Use Add action for each search, review or other task. Give it an owner, due date, status, outcome and evidence reference. Save case to preserve changes and obtain the permanent GDPR-A- action reference. Keep actual evidence of completed work in the restricted folder.

4 Response approval and closure

Record the decision and actual approval. Send the authorised response securely through the approved communication channel and retain delivery evidence; the case register does not send it. Complete or cancel outstanding actions with reasons, then record closure and retention-review dates. Save case again.

5 Saved change history

Review the saving account, time, revision and changed field names. History does not contain every earlier field value or prove response delivery. For a G1/G2 conflict, use View saved version separately to compare the newer record. Use Discard draft and reload saved case only after preserving any changes still needed, then reapply and save them. G5 does not provide these comparison controls.

6 Report and record a personal data breach

Report immediately if personal information may have been lost, stolen, wrongly disclosed, accessed without authority, corrupted or made unavailable. Examples include misdirected email, an exposed sharing link, a lost device, missing paper, accidental deletion or ransomware. Take only safe containment steps within your authority and preserve messages, headers, logs and other evidence. Do not erase devices without authorisation or circulate exposed records to explain the incident.

The lead assesses risk and records notification decisions. Where AIVS is controller, notify the ICO without undue delay and, where feasible, within 72 hours of awareness unless risk to people is unlikely. Where a breach is likely to create a high risk to people, affected people must be informed without undue delay unless a lawful exception applies. Where AIVS is processor, notify the client controller without undue delay; 72 hours is not a waiting period for notifying the client. Staff must report immediately rather than make these decisions themselves. [4]

Assigned incident handlers use the following G5 steps after making the direct report. Use categories, approximate numbers and restricted references rather than copies of affected records.

1 Create and save the incident

Open G5 Data breaches → Add breach record. Enter Breach title, Organisation, When you became aware (device local time) and What happened. Distinguish facts, estimates and unknowns; use the original awareness time and time zone. Save breach record and retain the GDPR-B- reference. For a G5 save conflict, preserve unsaved changes in the approved restricted incident file, reload the application, reopen the existing saved breach and compare before reapplying changes. Avoid creating a duplicate incident.

2 Record the risk decision

The Designated Director or alternate decides whether ICO notification is required. Record the assessment, decision, approver and reasons in the restricted incident file, with a reference in What happened. G5 has no separate approval or “not reportable” decision controls. An unticked ICO notification required box is not evidence of an approved decision not to report.

3 Prepare a notification when authorised

Tick ICO notification required to open ICO notification draft, or use Prepare ICO draft. Record the contact, people and records affected, risks, measures, notifications and any delay reason. Check the original awareness time: entry uses the device time zone and the calculated 72-hour deadline is displayed in UK time. The lead must verify the legal deadline; saving does not restart it.

4 Review and submit through the proper channel

Save and preview draft prepares the notification. Before using Email draft to me, enter Notification contact name and a valid Notification contact email. Email goes to the signed-in user, not necessarily that notification contact, and requires a configured email service. It does not notify the ICO. If emailing fails or is unavailable, use the saved preview without waiting.

The authorised lead must separately use Open ICO reporting form or another accepted ICO route and retain submission evidence. Do not wait for the investigation to finish. [4]

5 Follow up and preserve the outcome

Record actual notifications, updates, containment, corrective actions and closure in the restricted incident file; G5 has no separate action or closure workflow. Reference the saved breach record. Email-service acceptance is not proof of inbox delivery or ICO submission. Record every breach and the assessment, including a reasoned decision not to notify, with evidence of completed work. [4]

7 Review new processing suppliers and AI use

Before starting a new use of personal information, changing a system or introducing a supplier, seek the Designated Director's review. Confirm the purpose, lawful basis, privacy notice, access, retention, security and any overseas access or transfer arrangements. Follow documented client instructions when AIVS acts as processor; escalate instructions that appear unlawful.

Use personal or confidential information in AI tools only for an approved purpose in an approved service. Do not paste it into public AI tools or use it for model training without the necessary review and approval. Use synthetic or effectively anonymised data where practical and check outputs before use. Screen new or changed processing for privacy risk; a required DPIA must be completed before high-risk processing begins. [5]

8 Follow retention and deletion instructions

Follow the current approved retention schedule, client instructions and any legal hold. GDPR does not set one universal retention period. Do not keep extra copies just in case or delete records on your own when a request, complaint or incident is being investigated.

Carry out deletion only when authorised and record what was deleted, the authority, date and any retained-copy or backup limitations. Use approved methods for electronic and paper records. Escalate uncertain backup or supplier copies to the responsible owner. Keep minimal evidence of deletion rather than retaining the deleted personal information as proof.

9 Complete training and acknowledge these instructions

Complete the induction and updates required for your role, use the relevant HELP instructions and ask the Designated Director if unsure. Keep a dated record of the material and version, training completed, understanding checks, any gaps and agreed follow-up. Training records belong in the approved staff-awareness records; G1 Staff is a rights and complaints register, not the training register.

Check that you can explain what to do if you email a record to the wrong person, receive a verbal request for personal information or are asked to upload client information to a new AI tool. Report the first immediately, route the second promptly without requiring a form, and seek approval before the third.

Record acknowledgement of these instructions through the approved training process. Acknowledgement confirms receipt and responsibilities; it is not blanket consent to processing or proof that every training requirement has been completed.

Staff name | Role

Acknowledgement date | Record reference

Related instructions and sources

Document owner: Designated Director. Review when the law, software, reporting contacts or working practices change. Read with the current AIVS privacy notices and approved procedures. G1 to G5 and HELP instructions were checked against the supplied software on 31 October 2026; seek guidance if they change.

1 ICO personal information | 2 ICO subject access | 3 ICO complaints | 4 ICO breaches | 5 ICO DPIAs

UK GDPR and Data Protection Act 2018 guidance checked on 30 October 2026, including the current access-request and complaints guidance following the Data (Use and Access) Act 2025.