

AI DATA INCIDENT RESPONSE RECORD

Structured incident record for containment, supplier facts, risk assessment, notifications and corrective action

USE THIS WHEN INFORMATION MAY HAVE BEEN SHARED, UPLOADED, CONNECTED OR EXPOSED THROUGH THE WRONG AI SERVICE

Do not conceal the incident or erase key evidence before the facts are preserved. This form supports a structured assessment; it does not replace specialist advice for a significant or uncertain incident.

A. Incident reference and ownership

Field	Record
Incident ID	[]
Date/time discovered	[]
Incident owner	[]
Decision-maker	[]
Service / product / workspace	[]
User / account	[]

B. Immediate containment

Action	Time completed / evidence
Stop further sharing or activity	[]
Revoke public link / connector / access if still exposing data	[]
Preserve conversation/file ID, prompt, timestamps and visible settings	[]
Escalate internally to relevant owner/privacy/IT/engagement lead	[]
Submit supplier incident/deletion request if appropriate	[]

C. Establish the four facts

Fact	Record
What left?	Exact data categories; people/clients/customers affected; sensitivity; identifiers; attachments; re-identification risk.
Where did it go?	Product; plan/account/workspace; processing region; conversation/file ID; integrations; public/shared links.
Who could access it?	Supplier staff/reviewers; workspace users; subprocessors; public recipients; connected systems.
What happened next?	Training/evaluation use; retention; exports; downstream actions; deletion request; supplier confirmation.

D. Supplier questions

- Was the content used for training, evaluation or human review?
- Who or what accessed it, including subprocessors?
- Where was it processed and what residual copies/backups remain?
- Can the supplier confirm containment and deletion status with evidence?
- What incident or audit logs can the supplier preserve?

Supplier ticket / contact	☐
Supplier response summary	☐
Deletion / containment evidence	☐

E. Risk and notification assessment

Factor	Assessment / evidence
Sensitivity of information	[]
Volume / number of people	[]
Identifiability / confidentiality	[]
Recipients / access likelihood	[]
Likelihood of retrieval, misuse or downstream action	[]
Mitigations / containment already achieved	[]
Likely effect on people	[]

Notification decisions

Decision	Outcome / reason / approval / time
ICO notification required?	[Yes / No / Uncertain] - [reason]
Affected individuals notification required?	[Yes / No / Uncertain] - [reason]
Client/customer notification required contractually or professionally?	[Yes / No / Uncertain] - [reason]
Insurer / legal / professional-body advice required?	[Yes / No / Uncertain] - [reason]

72-HOUR POINT

Where a UK GDPR personal-data breach is likely to result in risk to people's rights and freedoms, regulator notification is required without undue delay and, where feasible, within 72 hours of awareness. Record the decision even where notification is not made.

F. Corrective action and closure

Action	Owner	Due date	Evidence / completion
Restrict or suspend tool/use case	☐	☐	☐
Reset account/workspace/settings/sharing	☐	☐	☐
Update tool/use-case register	☐	☐	☐
Update policy / wording / training	☐	☐	☐
Additional technical control	☐	☐	☐
Staff briefing / rehearsal	☐	☐	☐

Closure field	Record
Residual risk accepted by	☐
Closure date	☐
Evidence checked by	☐
Next review / follow-up date	☐
Lessons learned	☐

TEMPLATE STATUS

General information and an adaptable working record, not legal, data-protection or professional advice. Seek appropriate advice for significant, sensitive or uncertain incidents.