

Personal Data Breach Response Process

ProvisionIQ Ltd — Step-by-Step GDPR Breach Handling

Document	Personal Data Breach Response Process
Version	1.0
Date	22 May 2026
Owner	CTO
Legal obligation	UK GDPR Art. 33–34 · ICO Breach Reporting Guidance
Hard deadline	ICO notification within 72 hours (if notifiable)
Emergency contact	dpo@provisioniq.co.uk · security@provisioniq.co.uk

The 72-Hour Clock Starts When ProvisionIQ Becomes Aware

Under UK GDPR Article 33, the 72-hour notification deadline runs from when ProvisionIQ becomes aware of a personal data breach — not when the breach is confirmed or fully understood.

If in doubt whether a breach is notifiable: REPORT FIRST, refine later. The ICO accepts updates. Missed deadlines cannot be undone.

Where ProvisionIQ is the Data Processor, the 72-hour clock runs for the Data Controller (school/LA). ProvisionIQ must notify the Controller within 48 hours so they can meet their ICO deadline.

1. What Is a Personal Data Breach?

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data (Art. 4(12)).

Breach Type	Examples	Usually Notifiable?
Confidentiality breach	Pupil ISP sent to wrong parent; screen sharing exposed data; unauthorised staff access to records	Yes, if risk to individuals
Availability breach	Platform outage deleting data; backup failure; ransomware destroying records	Yes, if data lost permanently

Integrity breach	Data corrupted by bug; unauthorised modification of ISP records	Yes, if significant inaccuracy
Near-miss	Phishing email clicked but no data accessed; misconfiguration fixed before exploitation	Usually No (but log it)
Accidental disclosure (low risk)	Encrypted data sent to wrong recipient who couldn't open it	Usually No (but log it)

2. Step-by-Step Breach Response Process

Step	Action	Owner / Deadline
STEP 1 DETECT	Any person who discovers or suspects a breach immediately reports to security@provisioniq.co.uk. Include: what happened, what data, how many people, what actions taken.	Any Staff Member Immediately
STEP 2 TRIAGE	DPO and Lead Engineer conduct initial assessment within 2 hours. Confirm whether a personal data breach has occurred. Assign severity (P1–P4 per IRP classification).	DPO + Lead Engineer Within 2 hours
STEP 3 CONTAIN	Lead Engineer implements containment (per IRP Phase 3): isolate systems, revoke access, preserve evidence. DPO documents containment in Breach Register.	Lead Engineer + DPO Within 4 hours of detection
STEP 4 ASSESS	DPO completes Breach Assessment (Section 3 below): categories of data, number of individuals, likely consequences, measures taken.	DPO Within 4–8 hours
STEP 5 NOTIFY CONTROLLERS	If breach affects customer data: DPO notifies affected Data Controllers in writing. Provide: nature, scope, DPO contact, likely consequences, measures taken.	DPO Within 48 hours of awareness
STEP 6 ICO ASSESSMENT	DPO makes notifiability decision (see Section 4). If notifiable: submit ICO notification. If not: document the decision and rationale.	DPO Within 48–72 hours (hard deadline 72 hours)
STEP 7 INDIVIDUAL NOTIFICATION	If high risk to individuals: Data Controller (school/LA) notifies affected data subjects. ProvisionIQ provides draft letter, contact list, and support line.	Controller (school/LA) + ProvisionIQ support Without undue delay
STEP 8 ERADICATE	Technical team eliminates root cause. Vulnerability patched. Systems restored per DRP. DPO updates Breach Register with eradication details.	Lead Engineer + DPO Within 24–72 hours

STEP 9 FOLLOW-UP	PIR within 5 business days. Final breach assessment submitted to ICO if initial notification was incomplete. Written report to affected Controllers.	DPO + IC Within 5 business days
STEP 10 CLOSE	Breach Register entry closed. Lessons learned documented. Policy/process updates implemented. Insurance claim filed if applicable.	DPO + CTO Within 15 business days

3. Breach Assessment Form

Complete this form for every personal data breach (including near-misses). Store in Breach Register.
 Reference: INC-[YYYY-NNN].

Breach reference	INC-[YYYY-NNN]
Date/time detected	[DD/MM/YYYY HH:MM]
Date/time reported to DPO	[DD/MM/YYYY HH:MM]
Reported by	[Name and role]
Description	[What happened? How was it discovered?]
Data categories affected	[e.g. pupil ISP records, health data, safeguarding data, staff emails]
Approx. no. individuals	[How many data subjects potentially affected?]
Breach type	[✓Confidentiality / ✓Integrity / ✓Availability — tick all that apply]
Consequences	[Likely impact on affected individuals — risk to rights and freedoms]
Measures taken	[Containment, eradication, notification actions taken]
Notifiable to ICO?	[Yes / No / Uncertain] — Reasoning:
ICO notified?	[Yes — date/time: _____ / No — reason: _____]
Controllers notified?	[Yes — date/time: _____ / Not applicable]
Individuals notified?	[Yes / No / Not required — reasoning: _____]

4. ICO Notification Decision

The Three Questions

Q1: Has a personal data breach occurred? (destruction / loss / alteration / disclosure / access to personal data)

→ No → Not a breach. Log as near-miss. No ICO notification required.

→ Yes → Proceed to Q2.

Q2: Is the breach likely to result in ANY risk to individuals' rights and freedoms?

→ No (e.g. encrypted data; data already public; no sensitive data) → No ICO notification, but document decision.

→ Yes or unclear → NOTIFY ICO WITHIN 72 HOURS.

Q3: Is the breach likely to result in HIGH risk to individuals?

→ Yes (e.g. health data; safeguarding data; children's data; financial data; large scale) → NOTIFY INDIVIDUALS without undue delay (Art. 34).

→ No → Individual notification not required (but may still be appropriate as good practice).

ICO notification is made via: ico.org.uk/report-a-breach. Emergency ICO contact: 0303 123 1113. You can submit an initial notification with incomplete information and update it as you learn more — this is preferable to waiting for complete information and missing the deadline.

© ProvisionIQ Ltd 2026. Effective 22 May 2026. Registered in England & Wales, Co. No. 17240497