VERIVIUS

Sample policy template, generated 2026-05-31

Personal Data Breach Notification Policy

Sample policy template. This is a Verivius-authored template based on the verbatim text of the statutory source. Tenants adapt the operational sections to their own organisation. Where this template and the live regulation diverge, the live regulation wins.

Statutory anchor: UK GDPR Articles 33 and 34, UK General Data Protection Regulation (Retained Regulation (EU) 2016/679) **Primary source:** https://www.legislation.gov.uk/eur/2016/679/article/33 **Last reviewed:** 2026-06-01 **Verivius pack version:** v1.1, 2026-06-01

1. What the regulation says

> the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Commissioner
>
> The processor shall notify the controller without undue delay after becoming aware of a personal data breach.
>
> The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken.
>
> When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.
>
> The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3).
>
> the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption
>
> The full text of the regulation is at https://www.legislation.gov.uk/eur/2016/679/article/33. Where this policy and the regulation diverge, the regulation wins.

2. Plain British summary

A personal data breach is any security incident that leads to personal data being lost, exposed, altered or destroyed in an unauthorised way. When a breach happens, the controller (the organisation that decides why and how the data is processed) must assess the risk to the people whose data is affected. Higher-risk breaches must be reported to the Information Commissioner without undue delay and, where feasible, within 72 hours of becoming aware of the breach. If the risk to people is high, the controller must also tell the affected individuals in clear plain language. A processor (an organisation processing data on the controller's behalf) must tell the controller without undue delay; the controller then runs the assessment and the 72-hour clock.

3. Scope

This policy applies to all employees, contractors, and external parties at <provider name> who access, process, store, or transmit personal data (clinical records, staff records, billing records, supplier records, visitor records). It covers every IT system, every paper record, every device (laptops, phones, tablets, USB drives), every shared workspace (email, document storage, messaging), and every controller-and-processor relationship the provider operates.

(Tenant updates the angle-bracket placeholder.)

4. Roles and responsibilities

- **Registered Manager:** accountable for the data-protection system operating across every site. Reviews every reportable personal-data-breach record. Signs off the ICO notification before submission for breaches involving high risk to individuals.
- **Nominated Individual:** holds provider-side accountability for data protection.
- **Data Protection Officer (DPO; named where required under UK GDPR Art 37, or named voluntarily otherwise):** the day-to-day information-governance authority. Operates the breach-assessment routine, drafts the ICO notification, advises on processor contracts.
- **Information Governance Lead (where the DPO role is not required and not voluntarily filled; in small services often the Registered Manager):** carries the DPO-equivalent operational role.
- **All staff:** know how to recognise a personal-data breach (a lost laptop, a misaddressed email containing patient data, an unauthorised access event, a ransomware infection), raise the suspected breach to the DPO or IG Lead the same working day, do not delay.

(Tenant updates the named role-holders.)

5. Procedure

The personal-data-breach procedure operationalises UK GDPR Articles 33 and 34.

1. **Recognise and report.** Any staff member who suspects a personal-data breach raises it to the DPO or IG Lead the same working day. The clock for the 72-hour notification window starts when the controller becomes aware that a breach has occurred, not when the breach itself happened.
2. **Log the breach.** A breach record is opened with what happened, when it was discovered, what personal data was involved, how many data subjects are affected, the categories of data (personal, special category, criminal-conviction), and the initial known cause.
3. **Contain.** Immediate containment actions are taken: revoke compromised credentials, recover lost devices where possible, isolate affected systems, suspend the affected processor's access. Container actions are logged on the breach record.
4. **Assess risk to the rights and freedoms of natural persons.** The DPO assesses whether the breach is likely to result in any risk (notification to the ICO threshold) or high risk (additional notification to data subjects threshold). The assessment considers: severity and nature of the breach, type and volume of personal data, ease of identifying individuals from the data, severity of consequences, the special category or criminal-conviction nature of any data involved.
5. **Decide on ICO notification.** If the breach is likely to result in any risk to data subjects, the breach is notifiable to the Information Commissioner. The notification is made without undue delay and, where feasible, within 72 hours of awareness. Where the 72 hours cannot be met, the notification still goes in with reasons for the delay.
6. **Decide on data-subject notification.** Where the breach is likely to result in a high risk to data subjects, the controller must communicate the breach to the affected individuals in clear and plain language. The communication describes the nature of the breach, the likely consequences, the measures taken or proposed, and contact details for the DPO or IG Lead.
7. **File the ICO notification.** The DPO drafts and submits the notification through the ICO online system. The notification includes the categories of data subjects and personal data records concerned, the likely consequences, the measures taken or proposed, and the contact name for follow-up.
8. **Process-side review.** Where the breach involved a processor, the breach record references the processor and the processor's report. The DPA between controller and processor is reviewed for breach-notification obligations and timing.
9. **Closure with learning.** The breach record closes when containment is complete, notifications are filed, and any improvement actions are opened. The closure paragraph records what changed at the provider as a result.
0. **Pattern review.** The aggregate breach pattern (count by category, cause analysis, time-to-detection, time-to-containment) is reviewed at the monthly governance meeting.

6. Training requirement

- All staff complete UK GDPR awareness training at induction and annually. The training covers what counts as a personal-data breach, the 72-hour clock, the staff member's duty to raise the breach to the DPO or IG Lead immediately.
- The DPO and IG Lead complete role-specific data-protection training at appointment and continuing professional development annually.
- Any staff involved in handling special-category data (clinical staff, HR for occupational-health data) complete special-category-handling training at induction and every two years.

Training records held in the tenant's training matrix register.

7. Audit

Compliance with this policy is monitored by the DPO or IG Lead:

- **Per-breach review:** every breach is reviewed at closure for assessment quality, notification timeliness, containment effectiveness, and learning capture.
- **Quarterly breach-pattern review:** trailing-12-month view by category, cause, and detection lag. Patterns producing repeat causes are escalated as a system-level risk.
- **Annual policy review:** the policy is read against the live UK GDPR Articles 33 and 34, the Data Protection Act 2018, and any current ICO guidance on breach notification.

Audit findings recorded in the tenant's audit register; actions logged in the improvement-actions register.

8. Record-keeping

Personal-data-breach records are held for a minimum of 8 years from the date of the last entry per the NHS Code of Practice on Records Management and the UK GDPR Article 33(5) requirement for the controller to document any personal-data breaches. The Article 33(5) record must comprise the facts relating to the breach, its effects, and the remedial action taken; the documentation must enable the supervisory authority to verify compliance.

ICO notification correspondence and any data-subject notification correspondence are attached to the breach record and travel with it.

Verivius preserves the per-record audit trail indefinitely while the workspace is active.

9. Related policies in this pack

- Good Governance Policy (`hscra-reg-17-good-governance`)
- Statutory Notifications Policy (`cqc-reg-18-notification-of-other-incidents`)
- Safe Care and Treatment Policy (`hscra-reg-12-safe-care-and-treatment`)

10. Document control

Version	Date	Author	Changes
v1	2026-05-19	Verivius (sample)	Initial sample template.
v1.1	2026-06-01	Verivius (sample)	Filled out Sections 3 to 8 with concrete content. Section 4 names the DPO and Information Governance Lead roles with the breach-assessment and notification responsibilities. Section 5 expanded to a 10-step procedure covering recognise, log, contain, risk assessment, ICO notification decision, data-subject notification decision, ICO filing, process-side review, closure, pattern review. Section 6 names training tiers. Section 7 names the audit cadence. Section 8 references the NHS Code of Practice and the Article 33(5) documentation requirement.

This sample policy template was issued by Verivius as part of the Mock Inspection design partner onboarding pack. It is a template, not a substitute for legal advice or the tenant's own policy-development process. Where this template and the live regulation diverge, the live regulation wins.
