BoardCue Live Personal Data Breach and Security Incident Procedure

Version: 30 August 2026

Status: Operational procedure

1. Purpose

This procedure governs suspected or actual security incidents and personal data breaches involving BoardCue, including incidents affecting Customer Personal Data where ADEPTABLE acts as processor.

2. Immediate actions

1. Record detection time, source and affected systems.
2. Contain the incident without destroying necessary evidence.
3. Assess confidentiality, integrity and availability impact.
4. Identify affected organisations, data categories and likely scope.
5. Escalate to the incident lead and privacy/security owner.
6. Record the awareness timestamp once ADEPTABLE has sufficient facts to be aware that a personal data breach has occurred.

3. Customer notification where ADEPTABLE is processor

ADEPTABLE will notify the affected Customer without undue delay after becoming aware of a personal data breach affecting Customer Personal Data.

Where practicable, the operational target is an initial notice within 24 hours of awareness. The initial notice must not be delayed solely because root cause, full scope or all affected records have not yet been confirmed.

Information may be provided in phases. The incident register must record awareness time, first customer notification time and each material update.

4. What the initial notice should contain

- nature of the breach and affected service;
- discovery/awareness time;
- categories and approximate numbers of affected people/records where known;
- likely consequences;
- containment and mitigation already taken or proposed;
- contact point; and
- information reasonably required for the controller's own regulator/data-subject notification assessment.

5. Suspected incident not yet established as a breach

Not every alert starts the processor breach-notification clock. Suspected incidents must be triaged promptly. Where an incident is reasonably likely to cause material confidentiality, integrity or availability impact to Customer Personal Data, ADEPTABLE may provide an early security-incident notice while the breach assessment continues.

6. ICO and individual notification for ADEPTABLE controller breaches

Where ADEPTABLE is controller, the privacy lead must assess whether notification to the ICO and affected individuals is required under applicable law, record the decision and meet any statutory deadline.

7. Closure and lessons learned

- containment complete;
- required customer/regulator/individual updates completed;
- root cause documented;
- corrective actions assigned and tracked;
- security tests and DPIA/threat model updated where appropriate;
- supplier review completed where relevant.

8. Retention

Material incident and breach records should normally be retained for 6 years after closure, subject to legal hold and data minimisation.