Data Breach Policy

Top things to takeaway

Report Incidents Immediately

Suspected breaches must be reported without delay.

72-Hour Deadline

Notifiable breaches reported within seventy-two hours.

Everyone Has Responsibility

All staff must report data security incidents.

Customer First Notification

Controllers informed promptly after breach awareness

Risk-Based Notification Decisions

Notify ICO and individuals where required

Lessons Must Be Learned

Incidents reviewed to prevent future recurrence

Proprietary Notice

Version control and ownership

Policy owner: Kate Lincoln

Version no	Date	What changed	Changed by	Approver
1.0	06/02/2023	Approved version	Vicky Withey	DPO
1.1	12/08/2024	Annual review	Eddie Adams	DPO
1.2	12/03/2025	Rebrand	Eddie Adams	DPO
1.3	15/04/2026	Rebrand	Eddie Adams	DPO

What is this policy for?

This policy sets out Node4's approach to identifying, reporting, assessing, and responding to Personal Data Breaches and information security incidents involving personal data. It is designed to ensure timely notification to relevant parties (including customers as Data Controllers, and where required the ICO and affected individuals) in line with applicable Data Protection Laws, including the UK GDPR, and to support effective containment, investigation, recovery, and continuous improvement following an incident.

Who is this policy for?

This policy applies to all individuals who have access to Node4 information or process personal data on behalf of Node4, including employees, temporary/casual/agency staff, contractors, consultants, suppliers, and other data processors. It covers all formats of personal and sensitive data held by Node4 and must be followed whenever a suspected or confirmed incident could compromise the confidentiality, integrity, or availability of personal data.

Contents

Overview

This document sets out Node4's policy on the identification and notification of Personal Data Security Breaches to ensure compliance with applicable Data Protection Laws. Node4 Limited shall act with integrity and in compliance with the applicable law and regulations for the reporting of Data Breaches.

Background

Under applicable Data Protection Laws, organisations have a duty to report certain types of Personal Data Breaches to the ICO and in some cases to the individuals affected, notifiable breaches must be reported within 72 hours of being identified by the organisation.

The UK GDPR recognises that it will often be impossible to investigate a breach fully within that time-period and allows information to be provided in phases. Failing to notify a breach when required can result in a significant fine of up to £8.9M or 2% of global turnover.

Node4 (as a Data Processor) holds and processes data to meet the contractual obligations of its customers (as a Data Controller). Every care is taken to protect personal data from incidents (either accidentally or deliberately) and to avoid a data protection breach that could compromise security. Compromise of information confidentiality, integrity, or availability may result in harm to an individual, reputational damage, service provision, legislative noncompliance, and financial costs.

Scope

This policy relates to all formats of personal and sensitive data held by Node4. This policy applies to all employees at Node4 and includes temporary, casual or agency staff and contractors, consultants, suppliers and data processors working for, or on behalf of Node4. The objective of this Policy is to contain breaches, minimise the associated risk and consider appropriate action to secure personal data and prevent future breaches.

Definitions & types of breach

For the purpose of this policy, data breaches include both confirmed and suspected incidents. An incident is an event or action which, may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately and has the cause or potential to cause damage to Node4's information assets and/or reputation.

An incident can include:

- Loss or theft of confidential or sensitive data or equipment on which such data is stored (e.g. loss of a laptop, USB stick, iPad/tablet device, or paper record).
- Equipment theft or failure.
- Unauthorised use of, access to or modification of data or information systems.
- Attempts (failed or successful) to gain unauthorised access to information or IT system(s).

- The unauthorised disclosure of sensitive/confidential data.
- Website defacement.
- Hacking attack.
- Unforeseen circumstances such as a fire or flood.
- Human error – accidental disclosure, unsecure disposal of data.
- 'Blagging' offences where information is obtained by deceiving the organisation who holds it.

Reporting an incident

Any individual who has access to Node4's information is responsible for reporting a Data Breach or Information Security Incident immediately by raising it to Compliance Team compliance@node4co.uk or directly to the DPO (Data Protection Officer) at DPO@node4.co.uk. The DPO will be responsible for reporting the Data Breach to the ICO (Information Commissioners Office the UK's Supervisory Authority) if necessary.

Node4 (Data Processor) shall notify the controller (Customer) without undue delay after becoming aware of a Personal Data Breach. If a data breach occurs or is discovered outside of normal working hours, it must be reported as soon as it is practicable.

All Data Breaches will be reported within 72 hours (Article 33 – Notification of a Personal Data Breach) to the supervisory authority unless the Personal Data Breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification is not made within 72 hours, it shall be accompanied by reasons for the delay.

The incident report will include the following details:

- When the breach occurs (date, time, if known).
- If the data relates to people which is personally identifiable information.
- The nature of the information.
- How many individuals are involved or have been affected.
- An incident report form must be completed as part of the reporting process.

All employees should be aware that any breach of the GDPR Regulations may result in Node4's disciplinary procedure being instigated.

Containment and recovery

The Head of Quality with the DPO's assistance will first determine if the breach is ongoing to minimise the effect of the data breach. An initial assessment will be made by the Head of Quality, with the DPO, to establish the severity of the breach, Node4 will assist the Controller to establish recovery of losses and damage limitation. Node4 will establish a contact list of those to be notified during the initial containment. Advice will be sought in resolving the incident promptly and will determine the suitable course of action to be taken to ensure a resolution of the incident.

Investigation and risk assessment

An investigation will be undertaken by Node4 immediately and wherever possible within 24 hours of the data breach being discovered/reported.

Node4 will investigate the breach and assess the risks associated with it in conjunction with the Data Controller.

The report will advise of the severity, risk of occurrence and adverse consequences for the individual or company.

The investigation will include:

- The type of data involved.
- Its sensitivity.
- The protections are in place (e.g., encryptions).
- What has happened to the data, has it been lost, stolen, hacked, corrupted.
- Whether the data could be put to any illegal or inappropriate use.
- Who the individuals are, the number of individuals involved and the potential effects on those data subject(s).
- Whether there are wider consequences to the breach.

Notification

Node4, with assistance from the DPO, will determine the individuals for notification of the data breach, considering:

- Whether there are any legal/contractual notification requirements.
- Whether notification would assist the individual affected – could they act on the information to mitigate risks?
- Whether notification would help prevent the unauthorised or unlawful use of personal data?
- Would notification help Node4 meet its obligations under the seventh data protection principle?
- The dangers of over notifying. Not every incident warrant notification and over notification may cause disproportionate enquiries and work.

Notification to the individual whose personal data is affected by the incident will include a description of how and when the breach occurred, and the data involved. Node4 will offer clear advice on immediate and future protection including action taken to mitigate risks. Individuals will also be provided with the Controller's contact details for further information.

Node4 with assistance from the DPO may consider notifying third parties such as the police, insurers, bank or credit card companies, and trade unions. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future. Node4 will consider whether the Communications Team should prepare a press release and to be ready to handle any incoming press enquiries. All actions will be recorded by the DPO for the purpose of integrity and transparency of the investigation.

Evaluation and response

Once the initial incident is contained, the DPO will carry out a full review of the causation, effectiveness of the response and whether any changes to systems, policies and procedures should be undertaken. Existing controls will be reviewed to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring.

The review will consider:

- Where and how personal data is held and where and how it is stored.
- Where the biggest risks lie and will identify any further potential weak points within its existing measures.
- Whether methods of transmission are secure; sharing the minimum amount of data necessary.
- Identifying weak points within existing security measures.
- Staff awareness.
- Implementing a data breach plan and identifying a group of individuals responsible for reacting to reported breaches of security.
- If deemed necessary, a report recommending any changes to systems, policies and procedures will be considered by Node4.