Node4 Data Breach Policy

Data Protection GDPR

Public

Node4 Limited

15/01/2017

Node4 Data Breach Policy
In Accordance with GDPR

This policy shall document that Node4 Limited is firmly committed to conducting its operational activities in an entirely transparent, fair and honest manner. Node4 Limited shall act with integrity and in compliance with the applicable law and regulations for the reporting of Data Breaches.

The policy, which came into force on the 24th May 2018, shall be communicated to all employees and associated persons and shall illustrate and clarify the commitment made by Node4 Limited to ensure that policy is strictly adhered to.

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

Purpose

Node4 is obliged under GDPR to have in place a procedure to be followed to ensure consistent and effective approach is in place for managing data breach and information security.

Scope

This policy relates to all personal and sensitive data held by Node4 regardless of format. 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 any breaches, to minimise the risk associated with the breach and consider what action is necessary to secure personal data and prevent future breaches.

Definition/Types of Breach

For the purpose of this policy, data breaches include both confirmed and suspected incidents. An incident in the context of this policy 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 includes but is not restricted to the following:

- Loss or theft of confidential or sensitive data or equipment on which such data is stored (e.g. loss of 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;
- Blagging' offences where information is obtained by deceiving the organisation who holds it.

Node4 Limited | Millennium Way | Pride Park | Derby | DE24 8HZ | 0845 123 2222 | www.node4.co.uk

Reporting an Incident

Any individual who has access to Node4's information is responsible for reporting a Data Breach and Information Security Incidents immediately to the Compliance Manager and 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).

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 to within the 72 hours as per Article 33 – Notification of a personal Data Breach to the supervisory authority after having become aware of it, 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, itshall be accompanied by reasons for the delay.

The 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. (see Appendix 1).

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 DPO will first determine if the breach is still occurring. If so, the appropriate steps will be taken immediately to minimise the effect of the data breach. An initial assessment will be made by the DPO to establish the severity of the breach and who will take the lead investigating. Node4 will help the Data Controller to establish whether there is anything that can be done to recover any losses and limit the damage the breach could cause. Node4 will establish who may need to be notified as part of the initial containment and will inform the relevant parties where appropriate. 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 such as the potential adverse consequences for individuals, how serious or substantial those are and how likely they are to occur.

The investigation will need to take account of the following:

- the type of data involved;
- it's sensitivity;
- the protections are in place (e.g. encryptions);
- what's 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, number of individuals involved and the potential effects on those data subject(s);
- whether there are wider consequences to the breach.

Notification

The Node4 DPO will determine who needs to be notified of the data breach on a case by case basis with the following needing to be considered:

- 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 warrants notification and over notification may cause disproportionate enquiries and work.

Notification to the individuals whose personal data has been affected by the incident will include a description of how and when the breach occurred, and the data involved. Specific and clear advice will be given on what they can do to protect themselves and include what action has already been taken to mitigate the risks. Individuals will also be provided with a way in which they can contact the Data Controller for further information or ask questions on what occurred.

The Node4 DPO must 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. The Node4 DPO will consider whether the Communications Team should be informed regarding 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 causes of the breach; the effectiveness of the response(s) 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 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.

Appendix – Data Breach Reporting Form

Please act promptly to report any data breaches. If you discover a data breach, please, complete Section 1 of this form and email it to the Data Protection Officer (DPO@Node4.co.uk)

Section 1: Notification of Data Security Breach	To be completed by person reporting incident
Date incident was discovered:	
Date(s) of incident:	
Place of incident:	
Name of person reporting incident:	
Contact details of person reporting incident (email address, telephone number):	
Brief description of incident or details of the information lost:	
Number of Data Subjects affected, if known:	
Has any personal data been placed at risk? If, so please provide details:	
Brief description of any action taken at the time of discovery:	
For use by the Data Protection Officer	
Received by:	
On (date):	
Forwarded for action to:	
On (date):	

Section 2: Assessment of Severity	**To be completed by the Data Protection Officer in consultation with the Head of the area affected by the breach**
Details of the IT systems, equipment, devices, records involved in the security breach:	
Details of information loss:	
What is the nature of the information lost?	
How much data has been lost? If laptop lost/stolen: how recently was the laptop backed up onto central IT systems?	
Is the information unique? Will its loss have adverse operational, research, financial legal, liability or reputational consequences for Node4 or third parties?	
How many data subjects are affected?	
Is the data bound by any contractual security arrangements?	
What is the nature of the sensitivity of the data? Please provide details of any types of information that fall into any of the following categories:	
HIGH-RISK personal data □ **Sensitive personal data** (as defined in the GDPR Regulations) relating to a living, identifiable individual's a) racial or ethnic origin; b) political opinions or religious or philosophical beliefs; c) membership of a trade union; d) physical or mental health or condition or sexual life; e) commission or alleged commission of any offence, or f) proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.	
□ Information that could be used to commit identity fraud such as; personal bank account and other financial information; national identifiers, such as National Insurance Number and copies of passports and visas;	

□ Personal information relating to vulnerable adults and children;	

□ Detailed profiles of individuals including information about work performance, salaries or personal life that would cause significant damage or distress to that person if disclosed;	
□ Spreadsheets of marks or grades obtained by students, information about individual cases of	
student discipline or sensitive negotiations which could adversely affect individuals.	
□ Security information that would compromise the safety of individuals if disclosed.	
Data Protection Officer to consider whether further escalation is required	

Section 3: Action taken	**To be completed by Data Protection Officer**
Incident number	**e.g. year/001**
Report received by:	
On (date):	
Action taken by responsible officer/s:	
Was incident reported to Police?	**Yes/No** **If YES, notified on (date):**
Follow up action required/recommended:	
Reported to Data Protection Officer and Lead Officer on (date):	

Reported to other internal stakeholders (details, dates):	
For use of Data Protection Officer:	

Notification to ICO	**YES/NO If YES, notified on:** **Details:**
Notification to data subjects	**YES/NO If YES, notified on:** **Details:**
Notification to other external, regulator/stakeholder	**YES/NO If YES, notified on:** **Details:**