Node4’s commitment to GDPR Compliance Statement

What is GDPR?

The GDPR (General Data Protection Regulation) was set in place on the 25th May 2018, to strengthen, harmonise and modernise EU data protection law and enhance individual rights and freedoms, consistent with the European understanding of privacy as a fundamental human right. The GDPR regulates, among other things, how individuals and organisations may obtain, use, store, and erase personal data and will have a significant impact on businesses around the world. GDPR requires businesses to provide the necessary measures for controlling and processing personally identifiable data.

GDPR is a European privacy law approved by the European Commission in 2016 that replaced a prior European Union privacy directive known as Directive 95/46/EC (the “Directive”), which has been the basis of European data protection law since 1995. A regulation such as the GDPR is a binding act, which must be followed in its entirety throughout the EU.

What is considered “personal data”?

Personal data is any information relating to an identified or identifiable individual. This information can be used on its own or in conjunction with other data, to identify an individual. Personal data will now include not only data that is commonly considered to be personal in nature (e.g., social security numbers, names, physical addresses, email addresses), but also data such as IP addresses, behavioural data, location data, biometric data, financial information, and much more.

Whom does GDPR affect?

The scope of the GDPR is very broad and it will affect:

- All organisations established inside the European Union
- All organisations involved in processing personal data of EU citizens

The latter is the GDPR’s introduction of the principle of “extraterritoriality” which is where GDPR will apply to any organisation processing personal data of EU citizens, regardless of where it is established, and regardless of where its processing activities take place. This means that GDPR could apply to any organisation anywhere in the world, and all organisations should perform an analysis to determine whether or not they are processing the personal data of EU citizens. The GDPR also applies across all industries and sectors.

What does it mean to “process” data?

According to GDPR, processing is “any operation or set of operations which is performed on personal data or on sets of personal data; whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.” If an organisation collects, manages, uses or stores any personal data of EU citizens, it is processing EU personal data under the GDPR.

Does it matter whether you are a controller or a processor?

If you access personal data, you do so as either as a controller or a processor, and there are different requirements and obligations depending on which category you are in.

- A controller is an organisation that determines the purposes and means of processing personal data. A controller also determines the specific personal data that is collected from a data subject for processing
- A data processor is a person or organisation who deals with personal data as instructed by a controller for specific purposes and services offered to the controller that involve personal data processing

Do you need to comply with the GDPR?

All organisations should consult with legal and other professional counsel regarding the full scope of compliance obligations. If an organisation is organised in the EU or processes the personal data of EU citizens, then GDPR will apply to the business.

Node4's Commitment to GDPR

Node4 is committed to ensuring that our employees, customers, suppliers and all other stakeholders who we work with understand the importance of the General Data Protection Regulation (GDPR).

There are no specific standards for GDPR as it is a regulation. Node4 follows policies and procedures that are recognised by the UK's Supervisory Authority the ICO (Information Commissions Office) and follows ISO 27001 and the PIMS (Privacy Information Management System) Framework. Node4 is ISO 27001 certified by UKAS accredited auditors a copy of our certificate can be found here: https://www.node4.co.uk/hub/downloads/

Node4 implements, maintains and regularly tests its IT security practices, and can demonstrate to the ICO (Information Commissioner's Office) its ability to meet requirements set under the regulation.

Node4's Technical Management Group are focused on security measures which includes but not unlimited to; intrusion detection, firewalls, monitoring, restricted access, segregation of roles and responsibilities, protection of physical premises, hard assets, pre-screening of employees, data loss prevention and regular testing, monitoring and reviews.

Node4's Data Protection Framework

Data privacy is discussed internally and externally throughout Node4 with regular updates to the Board of Directors. Node4 has a Compliance Manager to assist with embedding data privacy into its operations through policies and procedures. The Data Protection Officer (DPO) is in place to protect the fundamental rights and freedoms of the individual to privacy and to be responsible for reporting any data breaches to the Board of Directors and the ICO.

GDPR Training and Awareness Programme for Node4 Employees

In June 2017, Node4 committed to Compliance Training for all employees to ensure that there is a clear awareness, understanding and guidance of GDPR. Employees must complete training on an ongoing annual basis.

GDPR for our Customers

At Node4 we have always honoured our customers' right to data privacy and protection. We have demonstrated our commitment by adhering to the current UK Data Protection policy, and we have revised our own internal policies to meet the requirements of GDPR.

We have always been committed to high standards of information security, privacy and transparency. We place a high priority on protecting and managing data in accordance with accepted standards. This includes our role as a data processor, whilst also working closely with our customers and partners to meet contractual obligations for our procedures, products and services.

What we are doing to help our customers at Node4 is to make them fully aware of our role in helping to provide the right tools, systems and processes to support our customers' need to meet GDPR regulations.

From April 2018, Node4 rolled out a change to our customers 'Terms and Conditions' to keep in line with GDPR. These clauses are standard, and we do not envisage them to change unless there is a change in laws or the regulation. Where customers hold personally identifiable information, it is for the customer to ensure that they have the correct security in place to protect their data and the legal basis by which, the customer uses that data.

Node4 as the data processor will carry out its contractual duties to meet customers instructions.

Node4 will assist customers with data subject access requests upon clear written instruction to the Helpdesk Support Team which can be contacted by email - support@node4.co.uk
Node4 will promptly inform the customer of any request for disclosure of the data from a data subject or any other third party, which Node4 receives directly and provide a copy of such request. Node4 shall not disclose or release any data without first consulting with and obtaining the consent of the customer, except where required by applicable law or any court of competent jurisdiction.

GDPR for our Suppliers, Third Parties and its Associated Business Partners

Due diligence prior to working with suppliers or associated business partners is completed by the supplier team to ensure that the organisation understands their roles and responsibilities under GDPR. Where appropriate, a privacy impact assessment will be completed, and evidence gathered.

GDPR for Node4 Marketing and Communications

Consent is changing under GDPR to be more explicit and transparent to the data subject on how personally identifiable information will be used and who it will be shared with. As part of Node4's compliance to meet this change, Node4 has updated its privacy policy which can be found here; https://info.node4.co.uk/hubfs/downloads/Node4%20Private%20Policy.pdf

How do you report a Data Breach?

Node4 has a data breach policy in place which can be found here; https://info.node4.co.uk/hubfs/downloads/Data%20Breach%20policy.pdf

If you need to report a data breach then please contact the Helpdesk Support Team by email support@node4.co.uk as soon as you are aware that a data breach has occurred.

Under GDPR, organisations have 72 hours to report a breach to the relevant supervisory authority (ICO Information Commissioners Office) https://ico.org.uk/for-organisations/report-a-breach/. Upon Node4 becoming aware of any loss, alteration, unauthorised disclosure of or access to the data, Node4 shall inform the customer without undue delay and shall provide all such information with full cooperation, as the customer may require to fulfil its data breach reporting obligations under Privacy Law.

Node4 will provide reasonable assistance to the customer in complying with any enquiry made, or investigation or assessment of processing initiated by the Information Commissioner. Node4 will be entitled to recover its reasonable costs of providing such assistance.

How can Node4 help you become GDPR compliant?

Node4 has identified many products and solutions which will help businesses mitigate the issues highlighted by specific GDPR articles and avoid the risk of the new GDPR legislation. Our experts can show you what key security tools you need to help protect your organisation's data.

Our services are positive steps which can assist in the due diligence to meet legislation criteria and provide control and management against many of the GDPR articles relating to securing data.

Of course, businesses still need to ensure that processes and procedures are still required to be assessed and checked against the new legislation by following the ICO's simple 12 step guide https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

Should you have any specific GDPR concerns that you wish to discuss, then please contact us at SalesSupport@Node4.co.uk

What happens if you do not comply with GDPR?

Non-compliance with the GDPR can result in enormous financial penalties. Sanctions for non-compliance can be as high as €20 Million Euros or 4% of global annual turnover, whichever is higher. For other breaches, such as failing to comply with articles under the regulation the authorities could impose fines on companies of up to €10m or 2% of global annual turnover, whichever is greater.