Empowering business to do more

UK GDPR Compliance Statement - Node4's commitment.

What is UK GDPR?

The UK 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.

The GDPR is retained in domestic law as the UK GDPR, but the UK has the independence to keep the framework under review. The 'UK GDPR' sits alongside an amended version of the Data Protection Act (DPA) 2018.

The key principles, rights and obligations remain the same. However, there are implications for the rules on transfers of personal data between the UK and the EEA.

There are also implications for UK controllers who have an establishment in the EEA, have customers in the EEA, or monitor individuals in the EEA. The EU GDPR still applies to this processing, but the way you interact with European data protection authorities has changed.

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.

Who does the UK GDPR apply to?
The UK GDPR also applies to controllers and processors based outside the UK if their processing activities relate to:

- offering goods or services to individuals in the UK; or
- monitoring the behaviour of individuals taking place in the UK.

All organisations should perform an analysis to determine whether they are processing the personal data of EU citizens. The GDPR also applies across all industries and sectors.

Do you need to comply with the UK 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 UK GDPR will apply to the business.

What does it mean to "process" data?
According to UK 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."

All processing is required to be lawful, fair and transparent and each purpose should be recorded to demonstrate lawful basis.

If an organisation collects, manages, uses, or stores any personal data of EU citizens, it is processing EU personal data under the UK GDPR.

There must be a lawful basis for processing data (Article 6) one of these must apply, consent, contract, legal obligations, vital interests, public task or legitimate interest.

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.

Node4's Commitment to UK GDPR
Node4 is committed to ensuring that our employees, customers, suppliers, and stakeholders understand the importance of the UK GDPR.

Node4 follows policies, procedures, and ISO 27001 and the PIMS (Privacy Information Management System) Framework which are recognised by the UK's Supervisory Authority the ICO (Information Commissions Office)

Node4 is ISO 27001 certified by UKAS accredited auditors a copy of our certificate can be found here: Resources - Node4

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.

UK GDPR Training and Awareness Programme for Node4 Employees

Node4 remains committed to UK GDPR and Data Protection training for all employees to ensure that there is a clear awareness, understanding and guidance. Employees must complete training at onboarding and as an annual refresher.

UK 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 Act 2018 , and have revised our own internal policies to meet these requirements.

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.

We support our customers at Node4 to be informed of our role in helping to provide the right tools, systems and processes to support their needs to meet UK GDPR regulations.

Node4 continues to amend and update the 'Terms and Conditions' to keep in line with UK 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 inform a customer of any request for disclosure of data from a data subject, or third party received directly by Node4. 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.

UK 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 UK GDPR. Where appropriate, a privacy impact assessment will be completed, and evidence gathered.

UK GDPR for Node4 Marketing and Communications
Consent is changing under UK 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

Once aware of a data breach please contact the Helpdesk Support Team by email support@node4.co.uk.

Under UK GDPR, organisations have 72 hours to report a breach to Information Commissioners Office (ICO)
https://ico.org.uk/for-organisations/report-a-breach/.

Node4 shall inform the customer of any loss, alteration, unauthorised disclosure or access to the data, and shall provide all information on request. The customer may be required and obliged to report a data breach, Node4 shall provide reasonable assistance to the customer in complying with enquiries, investigations or assessments of processing initiated by the Information Commissioner. Node4 will be entitled to recover its reasonable costs of providing such assistance.

Empowering business to do more

How can Node4 help you become UK GDPR compliant?
Node4 has identified many products and solutions which will help businesses mitigate the issues highlighted by specific UK GDPR articles and avoid associated risks. Our experts can show you what key security tools you need to help protect your organisation's data.

Our services provide positive steps to assist in the due diligence process, help meet legislation criteria and provide control and management against many of the UK GDPR articles relating to securing data.

Businesses can and need to ensure their processes and procedures are assessed and checked against the new legislation by following the ICO's guide-to-the-general-data-protection-regulation-gdpr-1-1.pdf (ico.org.uk)

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

What happens if you do not comply with UK GDPR?

Non-compliance with the UK GDPR can result in assessment notices, warnings, reprimands, enforcement notices and penalty notices (administrative fines). For serious breaches of the data protection principles, the ICO have the power to issue fines of up to **£17.5 million or 4% of annual worldwide turnover**, whichever is higher.

Source:
Guide to the GDPR 14 October 2022

A. Gilbert

Andrew Gilbert

CEO

06/02/2023