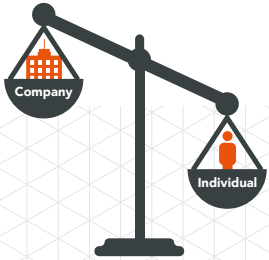
NODE4
enabling business to do business

GDPR in your Organisation

A 12 step guide to achieving compliance

From 25th May 2018, GDPR (General Data Protection Regulation) will place a greater emphasis on data controllers to be accountable for personal identifiable information that they hold. Organisations that suffer data breaches and fail to comply with the Regulation could face fines of up to 20 million euros or 4% of global turnover – whichever is greater. GDPR gives new rights to the individual to enquire and ascertain what information is held about them and how their data is used; shifting the balance of power from the company in favour to the individual. This simple 12-step checklist will provide you with a framework to review information and systems from collecting, processing, retaining personal information and how this is communicated and controlled within your business.



1. **What awareness is there in your organisation?**
Organisations need to review operationally how personal data is collected, processed and retained by involving key individuals from each department; in turn this will increase the profile of GDPR by engaging directly with the employees making them aware of the importance of compliance with the Regulation. Both communication and awareness will highlight how GDPR will affect your organisation and the challenges you may have around the privacy of data that you hold. Backing at board level will also need to be initiated to ensure that the correct resource and budget is allocated.

2. **What Information does your organisation hold?**
It is important to establish what personal data is captured, utilised, stored, who and how you share this information with be it internal and/or external. You will need to create a document showing the process flow of information within the business, and ensure that you have identified why information is collected, how it is collected and for what purpose. Confidentiality, integrity and availability of the information are the key questions to ask when identifying what information your organisation holds. In addition, documenting the process flow of personal data will comply with GDPR's six principles of accountability for data protection.

3. **How is your organisation going to communicate its privacy notices?**
Your organisation will need to update and display publicly your companies Privacy Notice explaining the legal basis for collecting and processing personal data and how long you will retain this information for. In addition, the Privacy Notice will need to include the DPO's (Data Protection Officer's) details, the Data Subject's rights and how individuals may correct inaccurate information or lodge a complaint against your business or the ICO if they believe that there is an issue with the way that you handle their personal data.

4. **Determine how your organisation is going to handle Data Subject access requests.**
Under GDPR, Data Subject access requests must be free of charge and may be made in any form; post, email, social media, telephone. Your organisation will have to complete the request within 30 days rather than 40 days previously. Verifying the Data Subject, that they are who they say they are presents its own challenges, so having the ability to 'stop the clock' when requesting further information will be imperative to adhering to the new timescales.
Knowing where to find the information quickly will be also be a huge benefit to meet the new Regulation and will save your business time, money and resources in managing such requests.

5 **Know what the Data Subject's rights are.**
You will need to understand how your organisation will uphold the rights for individuals when they make the following requests;

- The right to be informed about what personal identifiable information your business holds on them.
- The right to access the information.
- The right to rectify inaccurate information.
- The right to erase their personal information if there is no valid reason why your business needs to keep it.
- The right to restrict the processing of data.
- The right to data portability is new and corporates need to provide data in an electronic and commonly used format.
- The right to object to personal data being used, this is especially important when using data for marketing purposes that your organisation ensures that they have gained consent from the individual.
- The rights to challenge automated decision making and profiling.

"your organisation could risk fines of up to €20 million OR UP TO 4% OF YOUR ORGANISATION'S GLOBAL TURNOVER (whichever is greater!)"

6 **What is your legal basis for processing personal data?**
Your business will need to explain publicly the legal basis for processing personal data, which should be displayed within your Privacy Notice. If there is no legal or contractual basis for processing data then consent must be sought and evidenced from the individual.

7 **How is your organisation going to obtain consent from individuals?**
Your business needs to implement a process to clearly demonstrate documentation to obtain and record consent to keep personal information. Under GDPR, consent is a positive indication of agreement from the individual for their personal data to be processed and stored; consent must never be assumed.

8 **How is your organisation going to obtain consent from children?**
Your organisation needs to put in place a system to verify individual ages and to gather parental consent when collecting personal data from children. Consent must be verifiable and the privacy notice must be written in a language that a child will understand.

9 **How is your organisation going to manage a data breach?**
A data breach through identity theft, breach of confidentiality or a direct data leak, which may cause an individual any financial loss or personal harm, must all be reported to the ICO (Information Commissions Office) within 72 hours of the breach being identified. Failure to report a breach may result in further fines upon the business. Your business needs to develop and implement an incident management policy and procedure to handle data breaches to ensure that breaches are detected, reported and investigated in a timely and accurate manner.

10 **DPIA's (Data Protection Impact Assessments) will need to be carried out.**
GDPR makes DPIA's an express legal requirement and therefore, understanding how personal data is collected and the legal basis, how it is processed and stored are critical questions to answer when assessing the risk of confidentiality, integrity and availability of the information. All future projects that you carry out within your organisation will require a DPIA as part of the project process to comply with the new Regulation.

11 **Decide who will be your DPO (Data Protection Officer)?**
You need to ensure that someone in your organisation is responsible for data protection and compliance with GDPR, decide now who this will be and communicate this internally and externally. If your organisation is a public body, processes data on a large scale or collects and processes sensitive data then a DPO will be mandatory under the new Regulation and the ICO will need to be notified who the DPO is.

12 **Determine how your organisation may handle international transfers of data.**
If your organisation operates internationally outside of the EU then you will need to establish a process for transferring data securely.

0845 123 2222 | info@node4.co.uk | node4.co.uk