GENERAL DATA PROTECTION REGULATION

So what *is* GDPR?

Simply put, the GDPR is the first Data Protection Law to come out of the European Union and gives greater protection and rights to individuals.

What do you need to know?

If you handle personal data, or sensitive personal data, you need to know your legal obligations when doing so. Personal data is any identifiable data - from a name to an IP address. Sensitive personal data is religious and political views, sexual orientation and more.

The ICO says "If you are currently subject to the Data Protection Act, it is likely that you will also be the subject to the GDPR"

Don't panic!

The ICO has established clear guidelines, as well as some helpful myth-busting facts to help you navigate GDPR.

MYTH #1 Controllers don't need data processing agreements with processors because the GDPR imposes direct obligations on processors.

FACT Data processing agreements are vital to the controller and processor relationship as it binds both parties to specific terms. The Controller is ultimately responsible.

MYTH #3 Everyone needs a Data Protection Officer

FACT DPOs must only be appointed in the case of: (a) public authorities, (b) organisations that engage in large scale systematic monitoring, or (c) organisations that engage in large scale processing of sensitive personal data. If you don't fall into one of these categories, then you don't have to appoint a DPO - though appointing one is, of course, still to be encouraged in the interests of good practice!

MYTH #2 GDPR only applies to **PII** (Personally Identifiable Information)

FACT Personal data under GDPR applies to IP addresses and cookie tracking, too. It's important people treat **non-PII** (non-personally identifiable information) as personal data, too as any data that can be used to distinguish one person from another and can be used for de-anonymising anonymous data can be considered **PII**.

MYTH #4 Information on a business card is not in scope for GDPR.

FACT This raises other questions, like Is a business email address, such as info@, sales@, admin@, a personal identifier? Whilst the answer to this question is NO, the answer to the former is a resounding YES!

Information on a business card **is** all identifiable (PII) and therefore in scope of the GDPR – it is all identifiable information **(PII).**

12 STEPS TO TAKE NOW

Decision makers & key people need to be aware the law is changing to GDPR.

Document all personal data you hold, where it came from & who you share it with.

Review current privacy notices and plan any necessary changes.

Ensure procedures cover all rights individuals have.

Plan how you will handle subject access requests and update procedures.

Identify your lawful basis for processing personal data and update your privacy notices.

Review and update how you seek, record and manage consent.

Think about putting systems in place to verify age and obtain consent from parents or guardians.

Make sure you have the right systems in place to detect, report & investigate a breach.

Familiarise yourself with the ICO Code of Practices and latest guidance from Article 29 and how you implement it in your organisation.

Consider whether you need to formally designate a Data Protection Officer, if so, assess where this role fits in with your organisations structure and designate someone to take responsibility.

If your organisation operates in more than one EU member state, you should determine your lead Data Protection Supervisory Authority.

How can we help?

node IT SOLUTIONS

GDPR is more than just how you use and secure personal information, it's about your HR & Legal documentation processes and more.

We can help with your IT infrastructure and ensuring your digital environment is secure and we work with partners who can provide a full GDPR audit.

Get peace of mind today

e: gdpr@node-it.com
p: 01767 348 007
w: node-it.com/gdpr

GENERAL DATA PROTECTION REGULATION
GDPR READY