

What is GDPR? 6 question you need to answer before the deadline





Why is GDPR necessary?

Regulations such as GDPR have come about as a consequence of technology. The increasing storage of private data over decades has led to concerns over individual privacy. Technology has meant that there is a risk that privacy could be trampled on or sensitive user data accessed inappropriately.

Worst still data could be stolen and used for criminal activity. In essence, regulation ultimately is about protecting individual privacy and individual rights from abuse or misuse of technology.

Why has technology become a problem?

Technology has been deployed over the decades initially as a solution to a business problem. Latterly, technology has been deployed as a fundamental part of the business fabric without which

most businesses would cease to operate. In the age of digitisation technology in some instances is the business. Technology has however been deployed in a haphazard manner without security at its core and in many instances, organisations are playing catch up as opposed to having security as part of their core design.

So how is GDPR different to other regulations?

GDPR aims to compel organisations to protect individual privacy by ensuring that those handling the sensitive data are competent; only storing what data is essential, enforcing a policy that only allows access to the relevant people, and has systems in place to protect against and detect unauthorised access.

GDPR gives real teeth to data regulators in terms of enforcement powers including significant fines. It also extends responsibility globally to anyone who processes EU citizens data.

What do businesses need to do to comply with GDPR?

In order to comply with GDPR regulation, organisations need to do the following;

- Awareness—ensure everyone in your organisations knows about GDPR
- Information- document what personal data you hold and where
- Privacy and rights— ensure procedures cover individual rights
- Subject access requests— update procedures to handle access requests
- Lawful basis— identify your lawful basis for processing data
- Consent— review how you manage consent
- Minors— ensure you have consent for minors
- Breaches— ensure you have a plan and procedures to detect and report them
- Impact assessment— plan to undertake these in accordance with ICO guidelines
- Data Processing Officer— designate a DPO within your organisation

That is it in a nutshell. It is obviously much more involved in practice. The information commissioners website is a great resource for understanding what needs to be done and how to do it.

What are the benefits of becoming GDPR compliant?

Achieving compliance with GDPR will have a number of direct and indirect benefits. Firstly there will be a cost associated with achieving compliance which will likely involve resources of time and money.

Being compliant however is a strong indication that the organisation is processing data in a robust way compliant with best practices. This should mean that organisations are;

- More likely to protect sensitive data and thus individual privacy and rights
- Less likely to be breached as they will have better security in place
- Are more likely to detect security breaches
- Will be able to respond satisfactorily to individual's information requests

There is an increasing trend amongst organisations that are now requiring their supply chain to confirm their compliance with GDPR. This will become a differentiator enabling GDPR compliant organisations to be viewed more credibly.

What are the consequences of not complying with GDPR?

Non-compliance with GDPR can have quite severe consequences over time. This could include being excluded from business opportunities as well as the likely punitive measures that may result from an ICO investigation if an organisation has been found wanting in it's approach to

compliance.

Analysts are also predicting that after PPI claims expire next year, GDPR breaches will spawn a new chapter in the claims culture that could run for decades. Compliance with GDPR should be seen as a business opportunity and approached positively in terms of the benefits that it might bring to organisations.

Useful Resources

[GDPR Readiness Test \[Checklist\]](#)

[GDPR 12 Step to take NOW \[Infographic\]](#)

[9 Steps to Implement a Security Management Tool \[eBook\]](#)