London Management Consulting Factsheet

GDPR

What is GDPR?

The General Data Protection Regulation (GDPR) is the biggest change to data protection law for 20 years. Customers and employees now have more control over their data and what companies do with it.

GDPR applies to any data that can identify a living person, such as a name, email address, IP address, phone number, credit card number, or even just an online tag or username.

What do you need to know?

- know what information of this type you are holding
- know how it is processed and why, and where it goes
- be able to show that you have the owner's permission to hold it for these purposes
- be able to show that it is handled securely and is effectively protected
- be able to identify if you lose or mishandle it, and report this within 72 hours
- have someone specifically responsible for ensuring this happens

Why does it matter?

The fines for breaches can be up to €20 million or 4% of global turnover, whichever is the higher.

Customers and employees have the right to compensation for damages arising from a data breach, and so litigation will become more frequent and more expensive.

"If you think compliance is expensive, try non-compliance"

What sort of changes does GDPR require?

- Individuals have the "**right to be forgotten**" and the right to "**data portability**":
  - They can request that a company deletes all personal data and erases links etc.
  - They have the right to obtain a copy of all their data in a structured, commonly used and machine-readable format.
- Stricter **information security obligations** (both technical and organisational) apply to all companies that handle data, including their suppliers and sub-contractors. Companies need to make more rigorous checks of information security arrangements when engaging suppliers/sub-contractors, with a long list of provisions to be added to the contract.
- Data controllers must **notify the authorities of a security incident within 72 hours** of becoming aware of it. Depending on the type of incident, either all affected individuals (clients, staff etc.) must be notified individually, or a general public communication must be made. So incident response plans will be needed, and should be rehearsed.
- **Privacy** must be pro-actively factored into all new systems and processes that handle personal information.

What should you do now?

The General Data Protection Regulation (GDPR) came into force on 25 May 2018.

London Management Consulting is ready to help with GDPR understanding, preparation and compliance.

getintouch@l-m-consulting.co.uk www.London-Management-Consulting.com