

Becoming GDPR Compliant

What level is your business?

The GDPR comes in to play in the UK on the 25th of May 2018 taking over the Data Protection Act of 1998. Currently many businesses in the UK and Europe are unaware of what it takes to be GDPR compliant and with it fast approaching, businesses need to prepare to ensure they meet the compliance regulations.

This helpful checklist will help identify areas for improvement and prompt further considerations to ensure your business becomes GDPR compliant before May 2018.

DEVICE PROTECTION

	Answer
• Are your business hard drives encrypted?	YES NO
• Can devices such as phones, laptops and tablets be managed internally if they're lost or stolen?	YES NO
• Is your business using endpoint protection, so that only approved devices can be used with company devices?	YES NO
• Are all passwords you store managed by a third party secure system?	YES NO

CYBER SECURITY AWARENESS & TRAINING

• Does your business currently provide cyber security training to your employees?	YES NO
• Are your staff trained to identify phishing emails? Do you test them?	YES NO
• Are your staff aware of the most recent malware threats and how they might be delivered to the business?	YES NO
• Has your business got a process in place that can be activated if staff open malware?	YES NO
• Are all staff trained not to keep passwords or private data stored in personal folders on their computers?	YES NO
• Are your staff aware that they must report any financial, data, and confidentially breach to a member of management so they can report this to the ICO within 72 hours of loss?	YES NO

USER ACCOUNTS

Answer

- Do your staff have their own unique access rights and passwords, with appropriate permissions for their specific roles? YES | NO
- Do you have more than one method of authentication as well as a password, that is required to log in to your user accounts and email? YES | NO
- Do you have restrictions on the users that have local administration rights? YES | NO
- Are all passwords managed so they have to be a specific complexity? YES | NO
- If your business has employees who work from home, have you as a company made sure the computer/tablet they are using is safe and secure? YES | NO
- Within your server is each folder managed with restrictions for users who shouldn't have access to specific files? YES | NO
- When you obtain, a new customer does your business automatically sign them up for marketing emails? YES | NO
- Have you got a process in place whereby customers can easily opt out of marketing emails, additional services etc? YES | NO

BACKUP

- Do you have a secure backup and disaster recovery service in place for your business? YES | NO
- Do you have a daily backup in place? YES | NO
- Do you review your backup system every 6 months ensuring it's the right backup for you? YES | NO
- Do you maintain records of your company's processes? Making sure you document all personal and sensitive data held in the business, where it came from and who you intend to share it with? YES | NO

SECURITY PROTECTION FOR THE BUSINESS

- Has your business got industry standard Malware protection in place that detects and protects against Malware attacks? YES | NO
- Does your business have automatic updates turned on for all staff to ensure as a business you mitigate backdoor vulnerability issues? YES | NO
- Are your operating systems and servers up to date? Are you running on a system that is no longer supported such as windows XP or Windows Vista? YES | NO
- Have you got a secure Bring your own device (BYOD) policy in place for all staff and are they aware of the security threats that come with (BYOD) ? YES | NO

- Are you using a secure solution, developed for business to share files across the company? YES | NO
- Have you got more than one layer of security protection for your business to make your business more secure against Cyber Attacks? YES | NO
- Do you monitor your DNS? (Domain Name System) Does your current firewall/security system prevent IP Spoofing and threats? YES | NO

BUILDING SECURITY

- Does your office use a specific pin access or cards to allow employees or delivery men etc. in to the premises? YES | NO
- Do you have CCTV inside and outside the building? Do you have signs displaying 'CCTV in operation' outside the building? YES | NO
- Is your hardware secure in locked rooms, which is only accessible to dedicated members of staff or managers? YES | NO
- Do you have a separate guest Wi-Fi set up for visitors? YES | NO
- Do you change your Wi-Fi passwords regularly? YES | NO

How many did you answer 'yes' too?

Score
/34

Score >28

NEARLY THERE...

You are making great progress to GDPR compliance in regards to data protection but need to do a few more things.

Score >15-27

HALFWAY HOUSE...

You are on the right path to GDPR compliance in regards to data protection but need to do quite a bit more to get you on track.

Score <15

JUST STARTED...

You need to quickly make some changes to meet GDPR compliance in regards to data protection. There is a lot you can do to get on track.

Need help? Speak to our specialist IT Security Consultants

This checklist covers off the majority of areas for IT GDPR compliance. However, GDPR compliance applies across areas of the business not just IT. Scoring top marks on this checklist does not mean you are fully GDPR compliant.



www.infinitygroup.co.uk