GDPR COMPLIANCE

10 essentials to ensuring your compliance throughout the COVID-19 pandemic

Define employees' duties

☑ ☑ ☑ □

The most important action you can carry out is to outline your employees' roles and responsibilities by providing a clear-cut description of their everyday accountabilities. If you need your employees to follow a nine to five working day, be transparent about this. That said, it's best to foster independence by encouraging flexible working among your staff. By doing this, you're endorsing a performance-orientated environment in which efforts and results are given precedence.

Install encryption software

It's paramount you encrypt your remote workers' devices and implement data encryption on all devices. One option is to install an encryption software that encodes the entire desktop or only selected files. Or, install a remote-wipe app that deletes all data on a device if it gets lost or stolen, so if it falls into the wrong hands, the data won't be compromised.

Protect data with passwords

Make sure you implement strong password systems to guarantee data security within your company. Strong passwords should be applied to emails, work-related files and networks. Your remote employees can do this by following the below steps:

Create strong passwords that are distinctive, memorable and obscure.

Revise their login IDs on a regular basis.

Decrease the number of login attempts to three before blocking the login screen.

Enhance their protection by enabling a two-factor authentication.

Connecting to public Wi-Fi

Public Wi-Fi is convenient for remote staff, as it means they can work from wherever they like, including from home, cafes and co-working areas. But, if remote staff connect to public Wi-Fi without considering security, it can put data in danger. If you're concerned about your data security, you must state in your policy that employees aren't permitted to use public Wi-Fi. In the instance that your workers have no choice other than to connect to an unsecured network, ensure they keep file sharing to a minimum and use a VPN.

Review your policy

Ensure you tweak your policy once in a while to seal any security gaps and revise the regulations in line with your requirements.

Raise security awareness

You can strengthen your system by sending employees on training days or to workshops for a higher level of data security awareness. Other ways you can instil more understanding is by sharing blogs and podcasts that reveal authentic examples. For a bit of fun, you could introduce gamification to teach your development team about the importance of data security and GDPR compliance.

Implement a strong warning procedure

Should an employee encounter a data breach, there must be a clear, actionable procedure in place so employees can take the correct steps to report breach incidents to certified individuals. Your workforce must understand what signifies a data breach and what they can do if they notice one.

Provide a remote access policy

Devise a set of rules that clearly outline which employee has access to what. Make sure you obviously state the tasks and names of every individual that's entitled to log onto the organisation's servers. It's worth noting that none of your workers, whether based remotely or not, are allowed to have total access to your organisation's files or servers if they don't need them for their everyday duties. It's a good idea to limit specified sections of the site and permit your employees to access the data that's relevant to carrying out their daily job. Ensure you mention this within your policy.

Tips to avoiding fraud

Market-leading email security products do have additional measures to combat invoice fraud. However it's important to note, there is no silver bullet to prevent this type of incident occurring.

Training

Train and make your staff aware of these things. There are an abundance of resources to keep your staff up to date on the latest fraud techniques.

All organisations should implement IT Governance, with a minimum of cyber essentials. Call us today on **0207 317 4535** for a FREE consultation.

reflective
IT SOLUTIONS

☎ 0207 317 4535 ✉ support@reflectiveit.com 🌐 reflectiveit.com