Kogo

Sussex
Chamber of
Commerce

Top 10 Tips to Prepare Your Cyber Security for GDPR by Kogo Ltd

Under the GDPR, businesses face huge fines for data breaches, so it's vitally important you ensure your data protection and cybersecurity solutions! Here's our 10 tips on preparing your cybersecurity for the GDPR.

1. **Where is your data?**

Where is your sensitive data? Most will answer "In filing cabinets, and on our server.", but is that really the only place? Do you have a website that holds sensitive data, or a cloud application such as Sage 200 or Dropbox? The first step to protecting your data is knowing what there is to protect!

2. **Understand your "layers of protection"**

No tool is 100% effective. You cannot rely on just one thing alone; because any security can fail. Every additional layer of security you have hugely decreases the chances of a breach.

3. **Cloud-based antivirus**

Everyone has antivirus these days, but is yours good enough? Most antivirus is poorly equipped to deal with zero-day exploits and ransomware, both of which can cause huge data loss and interrupt your work.

4. **Get a hardware firewall**

Firewalls are important because they place a barrier between you and the attack, instead of trying to protect you from infections already on your system. But software firewalls still run on your system, so they have the same problem, and do not protect the network at all. A modern hardware firewall protects everything at once, and provides a physical layer of security between you and attackers.

5. **Trained staff are safe staff**

A huge risk vector are your employees. An employee leaving an unlocked device in public, or just incorrectly disposing of sensitive files, can be the start of a major data breach!

6. **Take control of your data**

If you have data with service providers, check with them that they are GDPR ready and what security they have in place.

7. **Get organisation-appropriate security**

Companies often use consumer-level software; and they are fine tools, but they are not good enough for your organisation! Consumer-level antivirus protects against threats consumers typically face; but not spear-phishing, CEO-fraud, metamorphic ransomware, or other targeted threats.

8. **Cyber Essentials Certification**

Getting Cyber Essentials Certified is an important step towards GDPR readiness. It not only highlights holes in your cybersecurity, but also proves you are working to protect your data, which helps mitigate fines should a breach occur.

9. **Develop a breach response plan**

Who takes charge during a breach? When do you inform ICO? With a breach response plan, a lot of the panic can be taken out of a breach, letting cool heads rule!

10. **Know how it works**

The GDPR is a complex set of regulations, and it's difficult to keep afloat of all of them! Do you need a Data Protection Officer? How does the GDPR affect you in light of Brexit? With such serious repercussions for failing to comply, we highly recommend speaking to experts on both the cybersecurity and legal/data protection fronts.

You can contact Kogo at 01342 333000 or askmartin@kogo.co.uk