Commercial Insurance Profile

June 2018

UK Businesses Grossly Unprepared for the GDPR

25% of organisations still don't know or are unsure where their personal data is held

71% of businesses still have not reviewed their privacy policy to ensure that it's GDPR compliant

79% of businesses still have not reviewed their data protection policy to ensure that it's GDPR compliant

Source: ThinkMarble

Provided by:
MacKay Corporate Insurance Brokers

01292 611 028

http://www.mackaycorporate-brokers.com

MACKAY
Corporate Insurance Brokers

Is Your Data Secure Enough For The GDPR?

Much to the dismay of many organisations, the GDPR is officially here. Despite having two years to comply, only 16 per cent of organisations are very confident in their GDPR preparations, according to a recent survey from the Institute of Directors. And, if there's one area that your organisation needs to be confident about, it's data security.

Under the GDPR, your organisation should have the following security measures in place:

- The personal data your organisation holds can be accessed, altered, disclosed or deleted only by those you have authorised to do so. In addition, those authorised individuals can only act within the boundaries that you have outlined for them.
- The personal data that your organisation holds is accurate and complete in relation to why you are processing it.
- The personal data remains accessible and usable. For example, if personal data is accidentally lost, altered or destroyed, you should be able to recover it and prevent any damage or distress to the affected individuals.

However, rather than providing a one-size-fits-all security procedure, the GDPR recommends that each organisation conducts a data protection self-assessment. It is important to realise that while your organisation's data security needs are unique, in general, you should have the following practices in place:

- Analyse the risks presented by your processing, and use this to assess the appropriate level of security you need to put in place.
- Draft an information security policy and implement it.
- Review your information security policies and measures on a regular basis and improve them if necessary.
- Put in basic technical controls such as those specified by established frameworks like Cyber Essentials.
- Use encryption and pseudonymisation where appropriate.
- Understand the requirements of confidentiality, integrity and availability for the personal data you process.
- Ensure that you can restore access to personal data in the event of any incidents, such as by establishing an appropriate backup process.
- Ensure that any data processor you use also implements appropriate technical and organisational measures.

If your preparations are less than sterling or there are gaps, you could be fined up to €20 million or 4 per cent of your annual turnover, whichever is higher. For more information on ensuring that your organisation's data security is GDPR compliant, contact MacKay Corporate Insurance Brokers today.

If You've Put Off Getting GDPR Compliant, Complete the Following 5 Documents ASAP

1. **Privacy notice/privacy policy:** Your organisation has a responsibility to provide individuals with information about why you are collecting their personal data, how you're collecting their personal data and how you're storing their data.

2. **Employee privacy notice:** You need to explain to your staff why you're collecting their personal data, how you're collecting their personal data and how you're storing their personal data.

3. **Data processing agreements:** If you work with a data controller or data processor, your relationship must be governed by a written agreement that includes a number of provisions to ensure GDPR compliance.

4. **Privacy impact assessments:** If you make any significant changes to your data processing arrangements, you will be required to conduct an assessment to identify potential risks.

5. **Internal data protection policy:** All of your employees that handle personal information need to understand how to comply with the GDPR, identify breaches and report such an incident.

Source: Information Commissioner's Office

Follow These 3 Steps to Stay Calm After A Data Breach

In 2017, 46 per cent of all UK organisations experienced at least one cyber-security breach or attack, according to government data. Under the GDPR, your organisation is required to report certain types of personal data breaches to the relevant supervisory authority within 72 hours. If you don't, you could be fined up to €10 million or 2 per cent of your annual turnover, whichever is higher.

To protect your organisation from hefty GDPR penalties, follow these three steps:

1. Contact the relevant supervisory authority of a breach within 72 hours.
2. Directly contact individuals affected by a breach if it is likely to result in a high risk to their rights and freedoms. (Note: The Information Commissioner's Office defines a high risk as 'the threshold for notifying individuals is greater than notifying the relevant supervisory authority'.)
3. Complete a breach notification containing the following information:
    - The categories and number of people affected by the breach
    - The categories and number of personal data records affected by the breach
    - The name and contact details of the data protection officer or an additional contact where more information can be obtained
    - A detailed description of the breach's potential consequences
    - A detailed description of what measures your organisation has taken or will take to address the data breach
    - A detailed description of the measures your organisation has taken or will take to mitigate any possible adverse effects to either itself or the individuals affected

Successful Strategies for Obtaining GDPR Consent

Your organisation's method of obtaining consent better be GDPR compliant. If not, you could be fined up to €20 million or 4 per cent of your annual turnover, whichever is higher. To ensure you're compliant, consider these strategies for obtaining consent:

- **Audit your mailing list.** Review your mailing list to identify whether you have a record of clients opting in. If you don't, remove that client. For new clients, have them double opt-in, which requires them to click a link to confirm that they knowingly have signed up.
- **Assess your current process for collecting personal data.** Evaluate whether your current process has an active and obvious opt-in. Additionally, keep well-organised records that clearly outline what individuals have consented to, what they were told, and when and how they consented.
- **Review what data you are collecting.** Re-examine the personal data you're collecting from clients and decide whether each item is necessary.
- **Integrate a pop-up on your website.** When visitors view your website's landing page, a pop-up should greet them and ask them to sign up for your mailing list.