Commercial Insurance Profile

May 2018

Is Your Privacy Notice GDPR Compliant?

If not, your organisation could be fined up to **€20 million** (roughly £16 million) or 4 per cent of your annual turnover, whichever is higher.

Source: EU Commission

Provided by:
MacKay Corporate Insurance Brokers

01292 611 028

http://www.mackaycorporate-brokers.com

MACKAY
Corporate Insurance Brokers

Don't Overlook Privacy Notices in Your Sprint to GDPR Compliance

The GDPR comes into effect on 25 May, which does not leave your organisation much time to comply. While you've most likely been busy making the necessary high-level GDPR revisions, such as to how you obtain clients' consent, you may be overlooking a key GDPR component—privacy notices. These notices provide data subjects, such as your employees, customers and prospects, with clear information on how their personal data will be handled and collected, and they are one of the quickest and easiest GDPR requirements to satisfy.

Unfortunately, even if your organisation already has a privacy notice, it most likely is not compliant with the GDPR. If you don't update your privacy notices, you could receive a fine of up to €20 million (roughly £16 million) or 4 per cent of your annual turnover, whichever is higher.

To help update your privacy notice, the Information Commissioner's Office (ICO) released a list of 10 things that must be included:

1. Identity and contact details of the data controller and the data protection officer
2. Purpose of the processing and its legal basis
3. The legitimate interests of the controller or third party
4. Any recipients or categories of recipients of the personal data
5. Details of transfers to non-EU countries and safeguards
6. Retention period or criteria used to determine the retention period
7. The existence of data subject's rights
8. The right to withdraw consent at any time
9. The right to lodge a complaint with a supervisory authority
10. The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences

This list forms the base requirements of what you must include in your privacy notices—be sure to seek out specific information from the ICO on GDPR privacy notices, as your specific circumstances may require more information.

Also remember that the GDPR says that the information you provide to people about how you process their personal data must be concise, transparent, intelligible and easily accessible. That means no jargon, that it's written in clear and plain language, and that it is free of charge.

For more information on complying with the GDPR, contact MacKay Corporate Insurance Brokers today and ask about our comprehensive GDPR Compliance Toolkit.

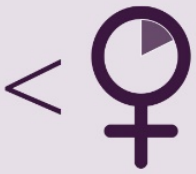
Snapshot of the Gender Pay Gap in the UK

- **78%** of companies pay men more than women

- **14%** of companies pay women more than men

- **8%** of companies reported no gender pay gap

- On average, women are paid **18%** less than their male colleagues



- Reporting companies averaged a **9.7%** pay gap

- **9 out of 17** sectors pay men, on average, **10% more** than women

- Construction had the highest gap with **23%,** followed by financial and insurance activities **(22%),** and education **(20%)**

- Accommodation had the smallest gap, with just **1%**

Source: Government Equalities Office

Minding Your Gender Pay Gap

Data from the first gender pay gap reports that were due 5 April have been released and the findings are disheartening. Organisations with at least 250 employees were required to disclose the pay gap between male and female employees, including their bonuses. According to the reports, 78 per cent of women work for organisations that pay them less than their male colleagues. What's more, women earn, on average, 18 per cent less than their male co-workers, while the average gap for the companies that were required to report was 9.7 per cent.

Closing the pay gap can be a challenge for any organisation. That's why the Government Equalities Office published guidance to help:

- **Calculate and publish your gender pay gap information, as required by law.** If your organisation is smaller than 250 employees, it would still be a good practice to collect this information to see what the gap is.
- **Analyse your data to learn where you can achieve the biggest improvements.** These changes could be made in recruitment, promotion rates as well as who's on your boards and executive committees.
- **Commit to an action plan.** Make a choice about how you will begin to close the gender pay gap and commit to it.
- **Monitor your progress.** Keep track of the effects of your action plan and make adjustments if change is not visible.

In addition to taking steps to address your gender pay gap, you may want to invest in employment practices liability insurance in order to shield you from harassment and discrimination claims. For more information, contact MacKay Corporate Insurance Brokers today.

GDPR Exposes Directors and Officers to Greater Risk

As cyber-related requirements will become more stringent under the GDPR once it comes into effect on 25 May, directors and officers (D&O) will be exposed to a greater amount of liability. In fact, insurance experts forecasted a spike in D&O claims in 2018 over cyber-incidents. But it's not just the GDPR—wrongful conduct resulting in company insolvency, such as Carillion's high-profile collapse, and equal pay issues highlighted by gender pay gap reporting could both contribute to a rise in D&O claims and a further widening of D&O liability.

To ensure that your organisation's directors and officers are prepared for this increased liability, consider making the following revisions:

- Ensure your D&O liability policy doesn't contain any specific exclusions about data breaches.
- Prioritise cyber-security at the highest level of your organisation by building cyber-governance into your organisational structure. Emphasise that cyber-security and GDPR compliance are the entire organisation's concern.
- Review your organisation's process for collecting clients' consent. Whatever your process may be, it must provide an active 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.
- Purchase D&O liability insurance to ensure your organisation's as well as your directors' and officers' well-being.