



Would your business survive a GDPR audit?

The European General Data Protection Regulation (GDPR) came into force in the UK on 25 May 2018 and, along with the Data Protection Act 2018, has brought considerable changes to data protection law, not only in the UK and across the European Economic Area, but also beyond as it significantly broadens the territorial reach.

The May deadline is now long gone and yet businesses around the world are still working to improve the way they handle personal data. As time goes on, regulators will expect more and more and indeed, GDPR is now an ongoing compliance risk to be monitored and assessed against. How would your business perform in a GDPR audit?

What are the risks of non-compliance?

The GDPR regime provides for significantly greater fines for breaches of up to €20 million, or 4% of the total worldwide annual group turnover, whichever is the greatest. Failure to comply with the GDPR also carries risk in the context of adverse publicity as it can lead to reputational damage and lost customer trust, civil liability or punitive damages for employment-related breaches, and business continuity issues. In addition, directors and managers can face personal criminal charges resulting in imprisonment and substantial penalties if found guilty of breaching the GDPR.

The Information Commissioner's office (ICO) has extensive and invasive powers to investigate and carry out audits. Whilst the ICO has said that it will be lenient with corporations as long as they can show they have taken steps towards compliance, we expect that they will look towards large multinational corporations based outside of the EU as a priority.

Who is caught by the GDPR?

Corporations will be caught by the GDPR if:

- They have a physical presence in the EU; or

- They are not EU based, but process data that relates to individuals in the EU, either in the context of offering goods or services, or by monitoring behaviour.

Data processing means holding, consulting and/or using information that makes any individual identifiable, directly or indirectly. All corporations process employee personal data, and most will also process personal data relating to clients, customers, suppliers and other contacts.

Data controllers and data processors

Whether you are data controller (meaning you decide the means and purpose of the processing of personal data) or data processor (meaning you process data on behalf of another corporation), you have increased responsibilities under the GDPR.

What's next?

Businesses should actively take steps to ensure that they are compliant. This involves training staff on new responsibilities, reviewing policies, systems and contracts as well as ensuring awareness of the transparency requirements.

Our team of GDPR experts can help you with:

- Completing data audits.
- Reviewing policies and procedures.
- Reviewing contracts.
- Staff training.

For more information on our GDPR services please contact:

***Steen Rosenfalck
Partner***

***T +44 (0)20 7553 9931
E sr@millerrosenfalck.com
I millerrosenfalck.com***

The material contained in this guide is provided for general purposes only and does not constitute legal or other professional advice. Appropriate legal advice should be sought for specific circumstances and before action is taken.