Herrington Carmichael
SOLICITORS

GDPR

Everything you wanted to know but never dared to ask

London
+44 (0) 203 755 0557

Camberley
+44 (0)1276 686 222

Wokingham
+44 (0)118 977 4045

info@herrington-carmichael.com
www.herrington-carmichael.com

HAVE YOU APPOINTED YOUR DATA PROTECTION OFFICER?

London
+44 (0) 203 755 0557

Camberley
+44 (0)1276 686 222

Wokingham
+44 (0)118 977 4045

info@herrington-carmichael.com
www.herrington-carmichael.com

Our guide to GDPR compliance

Businesses now rely on technology and the transfer of data online more than ever before, leading to an increased risk of data breaches occurring. This has led to an overhaul of data protection laws in Europe.

Europe's data protection laws will undergo their biggest change in two decades when the new General Data Protection Regulation (GDPR) comes into force on 25 May 2018. GDPR will replace the current UK Data Protection Act 1998, and will uniform data protection requirements across all EU member states.

Whilst this is considered an 'evolution', and not necessarily a 'revolution' of data protection laws across Europe, there are several significant changes for businesses.

Does this apply to me?

GDPR will apply to all companies, however big or small, that market goods or services to EU residents, even if a company does not have an establishment in the EU. Companies may, therefore, find themselves subject to the new regime even if they do not have a business presence in the EU, for example, technology companies.

What is personal data?

The GDPR applies to 'personal data', meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. GDPR broadens the definition of 'personal data' to location data and online identifiers, such as IP addresses and cookie data. 'Special categories of data' such as biometric and genetic data, which is become increasingly common for businesses to collect, will be subject to a higher standard under GDPR.

What is 'pseudonymisation'?

GDPR introduces the concept of 'pseudonymisation', which provides that personal data which has been pseudonymised, i.e. key coded, may fall outside the scope of GDPR if the pseudonym cannot be attributed to a particular individual.

Am I liable?

Data processors (responsible for processing data on behalf of a data controller, who determines the purpose and means of processing personal data) will now be directly liable for some matters which were previously only the data controller's responsibility. This is particularly significant as there will now be the possibility for individuals to enforce their rights directly against data processors.

What rights will individuals have?

Individuals will have greater control over their personal data under GDPR, such as objecting to their personal data being processed for direct marketing purposes and having their data erased in some situations.

Am I accountable?

Businesses will not just need to comply with GDPR, but will have to do so in a demonstrable manner. Policies and procedures must be documented, updated and impact assessments must be undertaken. Businesses will also need to consider privacy implications when designing new processes, products or services.

What are the consent requirements?

GDPR requires a higher level of consent, and businesses must obtain, freely given, specific, informed and unambiguous consent, with a clear affirmative action, i.e. an unticked tick box, to process that individual's data in certain circumstances. Consent must be easy to withdraw and explicit.

GDPR will dramatically increase fines for non-compliance. Companies violating GDPR may be fined up to €20 million or 4% of their global annual turnover, whichever is greater for smaller offences.

Is there a duty to notify a breach?

GDPR introduces a duty for businesses to notify a breach to their data protection authority, which is the Information Commissioner's Office (ICO) in the UK, within 72 hours after the company becomes aware of it. Companies must also notify affected individuals of the breach without undue delay, so internal procedures will be required for this.

What happens if I am in breach?

GDPR will dramatically increase fines for non-compliance. Companies violating GDPR may be fined up to €10 million or 2% of their global annual turnover, whichever is greater for smaller offences. For more serious offences, this is increased to €20 million or 4% of a company's global annual turnover, whichever is greater.

Do I need to appoint a data protection officer?

You must appoint a data protection officer (DPO) if you are a public authority, carry out large scale systematic monitoring of individuals, or carry out large scale processing of special categories of data or data relating to criminal convictions and offences. However, any organisation may appoint a DPO, taking into account an organisation's structure and size. Organisations who appoint a DPO will need to provide the DPO with the necessary training and resources to carry out his or her duties. The DPO must have a degree of independence and be the contact point for data subjects and the supervisory authority.

Is GDPR just another 'Millennium Bug'?

Unlike with the Millennium Bug, GDPR is known, and we know what is coming. The new legislation will happen, and it will come into force on 25 May 2018.

The data protection rules are sharpening under GDPR. The fines have increased, and the likelihood is that the currently low percentage of investigations which result in a fine will also increase. However, there is more to be concerned about than just fines. Judicial remedies are likely to be sought in respect of non-compliance, where damages could amount to much more than any fine, for example, the potential loss of share values in non-compliant companies. Media could also have a field day 'naming and shaming' organisations who are found non-compliant. Therefore, the safest thing to do with GDPR is to err on the side of caution. Businesses should ensure they have compliant policies and processes in place. In the event a case ends up in court, it will be in the company's favour to have shown willingness to comply with GDPR, even if it might not entirely eliminate a fine or pay outs.

In light of Brexit, will it even matter?

The report on 'Brexit: the EU data protection package' published by the UK Government on 18 July 2017 states that the Government is committed to ensuring that the UK remains 'a global leader on data protection' after Brexit. The Government has stated that it will continue to align its data protection framework with the EU to continue sharing personal data for commercial purposes, fighting crime and terrorism.

The Government has stated that it will continue to align its data protection framework with the EU to continue sharing personal data for commercial purposes, fighting crime and terrorism.

What should I do now?

Owing to the breadth of GDPR, businesses are advised to conduct an audit and a comprehensive review of data they hold and their existing data protection procedures to allow sufficient time and resources to affect the necessary changes required to ensure GDPR compliance.

10 STEPS TO BEING GDPR COMPLIANT

1. Learn about what is coming
2. Take stock of the data you hold and why you are holding it
3. Review the data you hold and the rights of the persons data you have
4. Inform the people about the data you hold on them, staff, clients or service users
5. Do you have the correct legal grounds to process data?
6. Do you have lawful consent - Get permissions!
7. Make sure you are aware of the ages of consent with regards the GDPR
8. Appoint a data protection officer
9. Plan ahead for any possible data breaches
10. Get a data protection impact assessment before a new project.

THERE IS STILL A TENDENCY WITHIN SOME BUSINESSES TO THINK THAT GDPR IS A ONE OFF PROJECT.

THIS IS NOT THE CASE.

GDPR: Here for the long-term

There is still a tendency within some businesses to think that GDPR is a one off project. This is not the case. Identifying temporary resource and allocating one off budgets to comply with GDPR will not make it 'go away.'

Getting ready for GDPR will mean implementing ongoing privacy governance, policies and processes, and continuously training staff on GDPR compliance. The business will then need to audit compliance and effectiveness on an ongoing basis. If a company's process for collecting data changes, policies and procedures will need to be updated accordingly.

For example, in commercial deals, data protection and privacy has gone from being a last minute, minor consideration, if a consideration at all, to a major hurdle to overcome in order to close a deal. Organisations who do not have appropriate measures in place in respect of data protection and privacy are finding it more difficult to close deals, or at least, to close them quickly.

In addition, the new and expanded rights under GDPR hugely increase the potential for data protection to be used as a weapon in the context of employment disputes. Data subject access requests, which often fill an employer with dread, can be time consuming, costly and a nuisance. These will not become easier to deal with under GDPR. The current fee of £10 will no longer be chargeable and employers will now have only one month to deal with a request.

However, the story does not start and finish with GDPR. There are other important ongoing developments in respect of privacy. For example, the e-Privacy Regulation will significantly impact any business operating in the online world as it will reform cookie consent requirements and communication privacy rules, so it is not all about GDPR. However, GDPR is the first step towards a significant overhaul in data protection and privacy laws globally.

Global Data protection

There has been an explosion in the number of countries in the world that now have data protection laws, and with the increase of globalisation, international data transfers have recently been under much scrutiny.

The US Safe Harbor scheme previously approved by the European Commission, which allowed data transfers to and from Europe and the US, is no longer valid. However, only 9 months after the invalidation of Safe Harbor, the EU-US Privacy Shield was adopted. The Privacy Shield is not referenced in GDPR, although GDPR does incorporate the key requirements assessing adequacy in terms of data transfers, as set out in the Schrems decision, which was the decision that put an end to Safe Harbor.

The EU Commission announced that it is reviewing the 'adequacy' status of countries currently deemed safe to receive EU data. This may introduce turbulence for international data movements, in addition to the increase in local data laws in territories such as China.

The world of data protection and privacy will become even more complicated for organisations operating on a global scale, particularly online businesses. There will be huge challenges ahead in meeting the laws of all the countries where businesses operate, with GDPR compliance as the first significant hurdle.

If you would like more advice about GDPR or appointing a Data protection officer, contact us:

London
+44 (0) 203 755 0557

Camberley
+44 (0)1276 686 222

Wokingham
+44 (0)118 977 4045

info@herrington-carmichael.com
www.herrington-carmichael.com

Herrington Carmichael
SOLICITORS

HAVE YOU APPOINTED YOUR DATA PROTECTION OFFICER?

Herrington Carmichael offer a range of high quality, plain speaking legal advice to businesses, individuals and families.

We believe in our traditional values of excellent service and value for money. Our clients appreciate our innovative, proactive and friendly approach. Our long-term client relationships are the very foundations of our 175 year old business.

Whether you are buying, selling, developing or leasing property, looking to secure your family's future, beginning, growing or protecting a business, or going through a difficult period, our teams are always available to support and advise you.

From our offices in London, Camberley and Wokingham we work with a growing number of clients in the UK and worldwide through our international network, IR Global. We have a historic connection with our local area as we look to consolidate our position as a leading law firm in Surrey, Hampshire and the Thames Valley.

London Office
Amadeus House, 27b Floral Street, London, WC2E 9DP
T: +44 (0) 203 755 0557

Camberley Office
Building 9, Riverside way, Watchmoor Park, Camberley, Surrey GU15 3YL
T: 01276 686 222

Wokingham Office
27 Broad Street, Wokingham, Berks RG40 1AU
T: 0118 977 4045

E: info@herrington-carmichael.com
W: www.herrington-carmichael.com