Briefing Note

The General Data Protection Regulation (GDPR)

From 25th May 2018, current data protection legislation will be replaced by the GDPR. With it comes stricter rules in relation to aspects of data protection such as how consent is acquired from data subjects and it places additional obligations on not only data controllers but data processors as well. All UK companies will need to be compliant with the GDPR by the time it comes into force, meaning time is running out but we can help.

1. GDPR: A Summary

1.1 The GDPR is European Union legislation that aims to do three things:

a) Update data protection law so that it adequately reflects a modern day, increasingly digitalised society;
b) Establish one set of rules that all applicable organisations need to comply with, replacing all of the various national laws that implemented the previous Data Protection Directive in different ways; and
c) Significantly strengthen the rights of an EU data subject in relation to how their personal data is collected and processed.

1.2 Personal data is defined as any information relating to an identified or identifiable natural person and is split into two categories: personal data and special categories of personal data. Special categories of personal data include racial or ethnic origins, political opinions, religious beliefs, genetic and biometric data, sexual orientation and health data. The GDPR makes it clear that online identifiers can be classed as personal data and this includes IP addresses, demonstrating that this legislation is geared towards protecting data in the digital age. All organisations that collect, use, and store, the personal data of any EU citizen will fall under the remit of the GDPR, even if that organisation is not based in the EU.

2. Some Key Changes

The GDPR introduces many changes to current data protection legislation, but some of the key ones are listed below:

2.1 **Data Protection Principles:** the GDPR has its own principles that will form the basis of lawful processing of personal data. Many of these are largely similar to the current principles under the Data Protection Act 1998 (DPA) but there are several differences and, importantly, the introduction of the "Accountability" principle. This requires organisations to not only be compliant with the GDPR, but to be able to demonstrate compliance as well.

2.2 **Territorial Scope:** the jurisdiction of the GDPR extends beyond that of the current Data Protection Directive. Although an EU regulation, it applies to all organisations that process the personal data of any EU citizen, regardless of where that organisation is located. This includes countries that are outside of the European Economic Area.

2.3 **Grounds for Processing:** The GDPR introduces six lawful grounds that organisations can potentially rely on to ensure that their processing of personal data is lawful:

2.3.1 **Consent:** where the data subject has given their consent to processing for one or more specific purposes. NB – there are specific rules regarding consent and direct marketing and we can advise on these;

2.3.2 **Contract Performance:** processing is necessary to perform a contract that the data subject is party to or in order to take steps at the request of the data subject prior to entering into a contract;

2.3.3 **Legal Compliance:** processing is necessary to comply with a legal obligation;

2.3.4 **Vital Interests:** processing is necessary to protect the vital interests of the data subject or another natural person;

2.3.5 **Public Interest:** processing is necessary in relation to the public interest or in the exercise of official authority. This is most applicable to public bodies and authorities;

2.3.6 **Legitimate Interests:** processing is necessary for the purposes of the legitimate interests pursued by the organisation or a third party, except where those interests are overridden by the interests, rights and freedoms of the data subject.

2.4 **Notification:** Currently, there is no legal obligation in England and Wales to inform either data subjects or the ICO that there has been a security breach relating to personal data. However, under the GDPR organisations that suffer a security breach will have to notify all data subjects affected by this and will have, at most, 72 hours from the time of the breach to notify the ICO as well.

Avoid the significantly increased "dissuasive" fines

3. Penalties for Breaches

3.1 One of the most important changes introduced by the GDPR is the fines that the ICO will be allowed to impose should there be a breach of the regulation. Currently, the maximum amount that the ICO can fine an organisation for a breach is £500,000. Under the GDPR this maximum jumps to €20 million or 4% of global annual turnover, whichever is greater.

3.2 Due to the significant increase in this enforcement power, it is crucial that your organisation becomes compliant as soon as possible and keeps on top of maintaining that compliance going forward.

An internal audit is the best starting point for compliance

4. Conclusion and Our Recommendations

4.1 All UK organisations will need to become compliant with the GDPR and there is still time to achieve this. If your organisation collects, uses, and/or stores personal data relating to EU citizens, then there are a number of recommendations that we would make to get you started on becoming compliant:

4.1.1 **Internal Compliance Audit:** Conduct an internal compliance audit, looking at the personal data you hold, the purpose for processing it, where it is stored, to whom it is transferred, and how long it is stored. This will help identify what gaps, if any, need to be rectified before the GDPR comes into force. We can provide guidance on this process;

4.1.2 **Policy Review:** Review your data protection policy, privacy notice and any related policies to see if they require updating. If you do not have any of these, you will need them drafted. We can assist you with this;

4.1.3 **Procedures Review:** Review your internal procedures that concern data protection. This includes procedures for collecting personal data, procedures concerning retention, and deletion of personal data, transferring personal data to third parties, and complying with data subjects' rights like making a subject access request;

4.1.4 **Contract Review:** Review your current contracts and agreements with third parties to whom you transfer and/or receive personal data to make sure that they are compliant with the GDPR;

4.1.5 **Training:** Make sure to arrange some training for your staff on the GDPR and what they need to do when dealing with personal data in order to be compliant;

4.1.6 **Security Review:** Review your security measures associated with data protection to see if they are adequate for the GDPR's requirements.

We can assist and advise on the above to help you become compliant and to demonstrate that you are compliant.

5. Contacts

5.1 If you would like to discuss the GDPR or any other matter mentioned in this Briefing Note then please contact:

Louise Purcell
Associate Solicitor
Whitehead Monckton
Direct Dial: 01580 767525

David Riordan
Associate Director
Whitehead Monckton
Direct Dial: 01227 643270

Drew Bailey
Solicitor
Whitehead Monckton
Direct Dial: 01622 698010

Maidstone Office
72 King Street
Maidstone
Kent, ME14 1BL

Canterbury Office
32-33 Watling Street
Canterbury
Kent, CT1 2AN

Tenterden Office
3-4 Market Square
Tenterden
Kent, TN30 6BN

Docklands Office
2 Beatty House, Admirals Way
Docklands Canary Wharf
London E14 9UF