GDPR factsheet

Key provisions and steps for compliance

Organisations hold vast amounts of personal data relating to customers, employees, and suppliers as well as within marketing databases. Compliance with data protection laws is vital in order to avoid sanctions, loss of revenue and negative publicity.

In this factsheet, we look at some of the key provisions in the new General Data Protection Regulation ("GDPR") that are relevant for your organisation. We also give advice on the steps that you can take now to gear up for compliance with GDPR.

GDPR snapshot

- The GDPR will apply from 25 May 2018 in the UK and across the EU.
- The GDPR will significantly impact the way in which businesses hold, store and use personal data.
- The "accountability principle" requires businesses to demonstrate compliance.
- Businesses will be accountable from day 1 and the fines are significant. Businesses therefore should start putting measures in place now.
- Regardless of Brexit, the GDPR is and will remain relevant to your business.

The following is intended to be a guide only to the GDPR and does not set out all the requirements and details. If you require any further information regarding GDPR please contact **Sarah Williamson** on **0118 952 7247** or email **swilliamson@boyesturner.com**.

Consistent with our policy when giving comment and advice on a non-specific basis, we cannot assume legal responsibility for the accuracy of any particular statement. In the case of specific problems, we recommend that professional advice be sought.

1. What is the GDPR?

The GDPR replaces the existing European Data Protection Directive and comes into force on 25 May 2018. It provides for the harmonisation of data protection legislation throughout the EU.

The European Commission's strategy in reforming European data protection laws was to create a "one stop shop" for data protection, with a common set of rules applying across Europe. This means that if you operate in a number of European countries you will only have to deal with one set of rules and one main Data Protection Regulator (in the UK this is the Information Commissioner's Office (ICO)). That said, there is not quite full harmonisation as there are a few areas where Members States have some discretion to legislate.

Consistency around data protection laws and rights should be of benefit to European businesses.

The data protection principles set out in the GDPR are to a large extent similar to those that we are familiar with in the DPA but there are additional requirements, the most significant being the "accountability principle" which means that data controllers are responsible for demonstrating compliance with the data protection principles. In addition, when we look at the possible penalties for failing to comply, the GDPR really does have teeth. Regulators will have enhanced powers of enforcement and the level of fines that can be levied is increased massively – €20 million or 4% of a company's worldwide annual turnover, whichever is greater. GDPR is not to be ignored!

2. What is the effect of Brexit?

Despite Brexit looming, the GDPR is still relevant for the UK for a number of reasons.

As the GDPR will apply from 25 May 2018, this will be before the UK exits the EU. You may process personal data relating to EU residents and therefore will have to comply with the requirements under GDPR, whatever the UK position.

The UK government's Statement of Intent on a new Data Protection Bill underlined that the GDPR is here to stay, even after Brexit. The full text of the Data Protection Bill was published on 14 September 2017 and this Bill will repeal the Data Protection Act 1998 and implement the GDPR in full to prepare the UK for when it exits the EU.

The Bill also deals with GDPR derogrations and includes the introduction of new criminal offences. The government has said that the new Bill will "allow the UK to continue to set the gold standard on data protection" so that consumers have "confidence that Britain's data rules are fit for the digital age in which we live".

So for anyone thinking that Brexit means that we can forget about the GDPR, this is not the case.

3. How does the GDPR apply to my business?

The GDPR will affect the way in which you go about your business and hold, store and use data about your customers, employees, suppliers and those individuals on your marketing databases. GDPR affects the notices and information that you will have to give to individuals about how their information is to be used.

The GDPR increases the power of individuals – including customers – to control, manage, inspect and, in some cases, delete forever, their information. The GDPR also gives individuals greater powers to complain about organisations which misuse their data.

The GDPR will affect businesses with US or non-EU parent companies as well as those with an EU presence.

Let's look at some of the key areas in more detail...

Key areas

- Expanded reach
- Consent
- Data subjects - Enhanced rights
- Data controllers - Governance and accountability
- Data processors - Direct obligations
- International data transfers

Expanded reach

The GDPR expands the reach of European data protection law and applies to:

- any organisation which has a presence in the EU that provides goods and services regardless of whether any payment is taken;
- any organisation which is based outside of the EU but which processes personal data of EU residents in connection with goods/services offered to him/her regardless of whether the processing takes place within the EU; and
- any organisation which monitors the behaviour of EU residents, e.g. the tracking of individuals online to create profiles and to analyse behaviours.

Therefore, it will not only be your European organisations that need to comply. If you have operations outside the EU which offer goods/services to EU residents, your non-EU operations will also have to comply with the GDPR.

Consent

The GDPR approaches consent more restrictively than the DPA.

- Consent must be **freely given, specific, informed and unambiguous.**
- Silence, inactivity and pre-ticked boxes are not sufficient. This may mean a change in the way in which you obtain consent for marketing activities.
- Explicit consent will continue to be required for the processing of sensitive personal data, e.g. data relating to racial or ethnic origin, mental or physical health, and religious beliefs.
- Separate consents are required for different processing activities and consent must be distinguishable and can't be bundled with other written agreements.
- The supply of goods and services can't be conditional on consent to processing where that processing is not necessary for the supply. So, the giving of consent for marketing cannot be a condition to, for example, booking a hotel room.
- There are greater controls over parental consents where children under 16 are asked to provide their data online. The GDPR doesn't set out the age at which a person is considered to be a child and Member States are able to set their own limit provided that it is not lower than 13.

Data subjects – Enhanced rights

Data subjects have a number of enhanced rights under the GDPR as follows:

- The right to be informed – you must provide information to an individual regarding the processing of personal data and the individual's rights.
- The right of access – you will no longer be able to charge £10 for a subject access request although you can charge a fee where the request is manifestly unfounded or excessive. You will have less time to comply with a request and information must be provided within one month of receipt of the request unless the request is complex, in which case, the period can be extended by two months.
- The right to rectification – an individual can request that personal data be rectified where it is inaccurate or incomplete and this must be done within one month unless the request is complex, in which case, the period can be extended by two months.
- The right to erasure – an individual has the right to request the deletion or removal of personal data in certain circumstances (e.g. the individual withdraws consent or the processing is no longer necessary) although this is not an absolute "right to be forgotten".
- The right to restrict processing – in certain circumstances an individual can require you to restrict the processing of personal data, e.g. where they contest the accuracy of the data or object to processing.

- The right to data portability – in certain circumstances an individual can request you to provide their personal data in a structured, commonly used and machine readable form and transmit this to a third party.

- The right to object – an individual can object to direct marketing (including profiling), processing based on legitimate interests or the performance of a task in the public interest/ exercise of official authority and processing for purposes of scientific/historical research and statistics. You must inform individuals of their right to object when you first communicate with them and in your privacy notice. For any online services, an individual must be able to object online.

- Rights in relation to automated decision making and profiling – an individual has the right not to be subject to a decision based on automated processing (which can include profiling) where it has a legal effect or a similarly significant effect on the individual.

Data controllers – Governance and accountability

The GDPR places onerous accountability obligations on data controllers to demonstrate compliance. One welcome change for data controllers is the removal of the notification requirement. However, there are a number of administrative burdens placed on data controllers. As a data controller your organisation will have to:

- Provide comprehensive, clear and transparent information to individuals regarding the processing of personal data and their rights;

- Maintain documentation regarding your processing activities;

- Implement technical and organisational measures to demonstrate that you have considered and integrated data protection into your data processing activities;

- Conduct privacy impact assessments (PIAs) where the processing is likely to result in a high risk to an individual's rights and freedoms;

- Appoint a Data Protection Officer (DPO) if your core activities require regular and systematic monitoring of data subjects on a large scale or the large scale processing of sensitive personal data or criminal records. The new DPO will have to have some knowledge about data protection laws and must report directly to the highest level of management. The DPO may be employed by your organisation or be a consultant and a group of companies may appoint one DPO responsible for the whole group; and

- Have processes in place for the notification of data breaches. Data breaches must be notified to the appropriate Regulator – in the UK, the ICO - without undue delay and, where feasible, within 72 hours of being aware of the breach. The threshold for notification to the data subjects themselves is where their rights and freedoms are placed at a "high risk". It is likely therefore, that all organisations will have to adopt some form of internal procedure for managing data breaches to avoid falling foul of these obligations.

Data processors – Direct obligations

The GDPR places direct obligations on data processors, which is a significant change. Data processors could include sales and marketing providers, cloud providers or other service providers which may process personal data relating to your customers, employees or suppliers.

The GDPR requires data processors to:

- Maintain records of personal data and processing activities;
- Notify data protection breaches; and
- Appoint a DPO if they fall within the threshold in terms of their processing.

It is important to note that the direct obligations on data processors do not relieve you as a data controller from liability as you have obligations under the GDPR to ensure that your contracts with data processors comply with the GDPR.

International data transfers

Transfers of personal data outside of the EEA have for a long time been an issue and the legal framework surrounding transatlantic data flows between the EU and the US was recently cast into uncertainty following the European Court of Justice's ruling that the US-EU Safe Harbor Framework is invalid. Those who had hoped for some clarity in this area are going to be disappointed as the GDPR does nothing to resolve the issues. Transfers of personal data to countries outside of the EEA continue to be restricted under the GDPR.

In July 2016, the European Commission approved the Privacy Shield framework for EU-US personal data transfers to replace Safe Harbor. This is a self-certification system and since 1 August 2016, US organisations have been able to self-certify. They must demonstrate the procedures they have in place to meet all the obligations under the Privacy Shield and the Privacy Shield Principles. The Privacy Shield is in place for an initial one year period with a joint annual review to take place in July 2017.

There are still other methods available for the transfer of personal data outside the EEA such as standard contractual clauses, binding corporate rules and limited exemptions, e.g. consent. However, some of these are also under threat of challenge and therefore the landscape for transatlantic data flows is by no means certain.

The important bit –

STEPS FOR COMPLIANCE

How do I prepare my business for the change?

Whilst the GDPR does not apply until May 2018, you should start taking steps now to ensure that you are ready. The accountability principle means that the onus is on you to be proactive in protecting individuals' data and avoiding breaches.

Here are some tips on the steps that you can take now:

Awareness and training - make sure that you and those in your organisation are familiar with the requirements of GDPR and look at rolling out a full training and compliance programme.

Audit – carry out an audit of the personal data that you hold. Track the data flows in order to identify what personal data you hold, where the personal data has come from, the legal basis on which you are holding it and where the personal data goes.

Privacy information and notices - review current privacy notices and put a plan in place to make any necessary changes.

Consents – check to see that if you are relying on consent for data processing that it meets the new requirements. If you use pre-ticked boxes to obtain consent for marketing information, this will need to be changed. Check your agreements with marketing agencies and list brokers to ensure that any marketing they carry out on your behalf or marketing databases that they provide to you meet all the necessary requirements.

Contract documentation - audit any existing supplier agreements that you have in place and update data processing/protection provisions in your standard agreements and tender documentation.

HR policies and employment contracts – review existing HR policies and documentation to ensure that you meet all the requirements of GDPR in relation to your employees.

Check procedures – check your procedures to ensure that they allow for compliance with the data breach notification requirements as well as all the new applicable rights conferred to individuals under the GDPR, including the deletion or removal of information and subject access requests. You will need to work with your IT team to ensure that your organisation has appropriate technical and organisational measures in place and that any marketing suppression processes operate in compliance with GDPR.

Privacy Impact Assessments (PIA) – identify whether you need to carry out any PIAs and familiarise yourself with the requirements.

Data Protection Officers (DPO) – either appoint or train an individual in your organisation to take responsibility for data protection compliance and this is advised even where you don't need to appoint a DPO. Ensure that management is aware of the importance of this role.

Cross border operations – if you operate in more than one European country, decide which is the relevant data protection authority for your activities. Also if you transfer or process personal data outside the EEA, you need to identify the mechanism that you rely on to do so and watch out for any changes that may occur over the coming few months/years regarding cross-border data transfer.