DATA PROTECTION

The mere mention of the General Data Protection Regulation is enough to send many a HR director, or data protection officer into panic. In order to combat this, we will give you an overview of the implications of the General Data Protection Regulation (GDPR) for businesses. We will discuss the likely timing of the implementation, look at the enhanced rights of data subjects and the new obligations on businesses as data controllers and we will conclude by considering appropriate steps that businesses can take in order to prepare for the introduction of the Regulation.

Background

After a four-year gestation period, the text of the GDPR was formally adopted in April 2016 but it does not take effect until 2018, when on 25 May the GDPR will replace our own domestic Data Protection Directive.

This gives us just over 12 months to prepare for the changes.

Common principles

The GDPR definition of personal data is very similar to the one we currently have under the Data Protection Act.

Simply, **personal data** is 'any information relating to an identified or identifiable natural living person'.

Therefore:

1. data held on a person who has **already been identified** is personal data; and
2. data held on an individual **who can *be* identified** is personal data.

This usually encompasses names and addresses of staff, volunteers and donors, but it can also include more general information about the physical, genetic, cultural or social identity of a person. Remember - it can also include data which appears to be anonymised - such as job titles - 'head of IP at Paris Smith' identifies me personally if you type it into google or look on our firm website.

The GDPR retains definitions that we are already familiar with:

- A **data controller** is an individual or legal entity which **controls** how and why the personal data is collected and processed. This is most commonly the EMPLOYER/BUSINESS.
- A **data processor** is the individual or legal entity which **processes** the personal data *on behalf* of the data controller – (sometimes this can be the same entity but is often an independent legal entity to whom the processing function is outsourced).
- The **data subject** is the **individual to whom the personal data relates**. This is usually the EMPLOYEE.

The general approach of the GDPR is similar to that of the current Data Protection Directive in that the GDPR requires data controllers to comply with a set of principles for processing personal data.

A data controller must ensure that it can meet **at least one** of a number of gateway conditions providing the legal basis for processing and in doing so, **it must give data subjects information on its purposes.**

GDPR - What's new?

When it comes into effect in May 2018, the GDPR will introduce a range of changes.

1. There will be **no more notification requirement** – the current rules require data controllers to register with the ICO. This notification requirement is being abolished going forward.

2. **Scope of protection** – The new rules will extend to data controllers and processors who offer goods and services into the EU but themselves are based outside of the EU. This is not the case under the current rules where businesses are only bound by Data Protection legislation if they are based within the EU. This means that even in a 'hard Brexit' scenario, the new rules will affect many British businesses if they are processing data pertaining to individuals based within the EU.

3. **New Duties for Data Controllers** - Looking specifically at the new duties for data controllers under the GDPR. The main changes are with regard to focusing on;

a) demonstrating compliance. As we are all very aware already, as data controller, the business has a duty to comply with data protection principles. However the GDPR also requires the data controller to be able to demonstrate compliance through rigorous **documenting decision making processes and following documented procedures.** It will not be sufficient to say "but we are not in breach and therefore must be compliant"; compliance must be actively undertaken and it may be necessary to implement new technical and organisational measures to show compliance.

b) **data protection by design** - from May 2018 ALL data controllers will be expected to take steps to build data protection into system design.

Subject to what is technically practicable and subject to cost, businesses will need to build in safeguards to comply with the new rules. Measures must be taken to:

1) minimise data collected;
2) ensure it is processed ONLY for the specific purpose for which it was obtained; and
3) ensure that the data is retained for no longer than is strictly necessary in the circumstances.

c) **impact assessments** - the GDPR will introduce obligations on data controllers to undertake 'regular' impact assessments of high risk processing activities. How regular these assessments need to be is not yet clear, but it is anticipated that the assessments should really be 'ongoing' and certainly annually. The assessment should include:

- a description of any high risk processing activities;
- the purpose for which the activities are being carried out;
- identification of any risk arising from the processing; and
- identifying measures being taken in order to mitigate against such risk.

4. **New duties for data processors** - data processors don't get away with it!

Businesses typically use data processors in a number of contexts, including banking, often outsourced HR and payroll function and as a provider of cloud services.

a) The GDPR tightens the rules on the use of data processors, extending the formal contractual requirements needed between data controllers and processors. From May 2018, the third party processor may only process personal data if it has documented instructions from the data controller setting out the specific processing activities to be undertaken.

b) The data processor will be under an obligation to notify the data controller of any data breach of which they become aware. The failure to do so is going to incur a liability and it is no longer enough for the data processor to hold their hands up and say 'we were acting on instructions'. The data processor will have to be accountable for its own actions and will be under an obligation to demonstrate compliance to the controller.

As a result, it is likely that data processors will seek to limit their risks by wanting greater clarity on their responsibilities. In light of this, engaging a processor for anything more than a simple task is likely to become more complex.

5. **Fair Processing Notice**

Under the existing law, data controllers are required to

provide individuals with a privacy notice (sometimes called "**Fair Processing Notice**") setting out the purposes for which data is processed, together with any further information needed to ensure processing is fair and legally compliant.

Under the GDPR, all information provided must be:

- concise
- transparent
- easily accessible and
- given in plain language.

In addition, data controllers will need to explain:

- where the data has originated from (unless it originates from the data subject);
- who will receive personal data (or the categories of recipients);
- the period for which data will be stored; and
- businesses will have to inform the individual of the existence of extended data subject rights (see below);
- whether the data is being transferred outside of the EU - remembering that this is going to be us in two years time. If data IS being transferred outside of the EU, businesses are going to be required to provide individuals with information concerning the legal basis for the transfer of the data to a non-EU third country **and**, give information on the safeguards applied to the transfer of such data.

It seems apparent that businesses will need to provide significantly more information than is required at present under the DPA. Accordingly, there is a risk of tension between the level of detail required to be supplied and the obligation to provide information concisely, accessibly and in plain language and we look forward to yet more guidance on this in due course.

6. **Data Subject Rights**

a) The data subject access right (**DSAR**) in Article 15 of the GDPR is broadly similar to the rights under the existing rules. However, the GDPR introduces additional rights for data subjects which include a package of new rights broadly summarised as 'delete it freeze it correct it' including:
   1) the right to be forgotten – which might be exercised where for example:
      the processing of data is no longer necessary in relation to the purposes for which it was collected or processed.
   2) the right to rectification – where for example the data is inaccurate or incomplete and
   3) the right to restriction of processing (Article 18) – where the processing is either unlawful, or where a data subject has objected to processing based on the 'legitimate interest' condition.

b) The current compliance period for responding to a data subject access request is **40 days** and this will be replaced with an obligation to comply **without undue delay and within one month, with an extension of two additional months if necessary**, taking into account the complexity of the request.

   Given the complexity of most DSARs in a commercial context, it seems likely that the normal period for compliance will be up to three months almost as a matter of course provided that your decision making process for extending this time frame is clearly documented.

c) The current £10 fee applicable to requests under the Data Protection Act 1998 will be abolished. However, where a request is "manifestly unfounded or excessive" the employer may either charge a "reasonable" fee, taking into account administrative costs.

d) Or the data controller **may refuse to act on the request altogether**.

   Clearly this is a significant change and a refusal to act altogether is not something to be used lightly - such a refusal will require clear and justified reasoning which must be fully documented.

What is "manifestly excessive" will depend on the specific circumstances, but it is hoped that the ability to either charge a reasonable fee or refuse to act altogether COULD have the potential to discourage vexatious and onerous requests.

It is intended that where requests are substantial, the revised rules should lead to a dialogue between the Business and the data subject. This should lead to clarity on what information the data subject wants and how to handle the request, with the fall back of the regulator if either side is being unreasonable.

If nothing else, the new rule should inhibit requests encompassing thousands of emails requiring days of work from a team of people.

7. **Consent**

Looking at a few key areas in more details - the giving of consent by a data subject is one of the gateways (and is the least controversial gateway) through which a business can establish a legal basis for processing personal data.

As you might expect, the GDPR sets out stricter and more detailed conditions for the obtaining of consent:

- The onus is on the business to show that consent has been given and such consent must be freely given, specific, informed and unambiguous.
- It will not be considered freely given if there is no genuine free choice.

At present, many businesses obtain consent for processing personal data by the **use of standard provisions** in either their employment contracts (in respect of employees or volunteers) or standard forms in respect of donations received. In general, standard forms are offered on a "take it or leave it" basis, under which an individual has no real choice. This means the consent obtained in the contract is unlikely to be effective from May 2018.

The ICO suggests that if consent is given by means of a written declaration, the request must be made in a manner that is clearly distinguishable from other aspects of the document. The ICO is currently recommending that the individual gives specific consent using a separate signature box.

- As is currently the case, an individual has the right to withdraw consent at any time but the GDPR requires that he/she must specifically be informed of this right by the business. The principle is that **it must be as easy to withdraw consent as it is to give it.**

8. **Data Protection Officers**

Although some businesses will appoint DPOs voluntarily, there is only a requirement to have a DPO under the GDPR if your core activities involve:

- systematic monitoring; or
- large-scale processing of sensitive data (for example, health data or criminal records); or
- if you are a public body.

Data processors will also be required to appoint a DPO if processing is carried out by them on behalf of a public authority or body.

There are no set rules as to a job description for a DPO but using common sense - some of us solicitors, do have some, = the main roles of a data protection officer (DPO) are to:

1) advise data controllers or data processors of their legal obligations;
2) monitor compliance with the GDPR;
3) be responsible for the implementation of policies, undertaking impact assessments and data protection by design; and
4) be a point of contact for the regulator.

A DPO will be independent, with a position in some ways analogous to an auditor although it is perfectly permissible for the DPO to be an employee.

9. **Data Breach Notifications**

The definition of a **personal data breach** is "*a breach of security leading to the accidental or unlawful destruction, loss, alteration or unauthorised disclosure of personal data*".

Employees and volunteers, despite being the most wondrous of people, can make mistakes; they leave laptops on trains (if they work for banks it seems), send emails to the wrong person and are careless with passwords. These are all personal data breaches.

Under the revised rules, employers discovering a personal data breach must notify the regulator promptly and **within 72 hours**, if feasible. If the notification is not made within this time, the employer must provide a "reasoned justification" explaining the delay. The notification requirement does not apply if the breach is unlikely to result in a risk to data subjects (for example, because all data on a laptop was encrypted).

In notifying a breach, a business must describe:

1. what has happened; and
2. set out the approximate numbers of individuals affected;
3. the likely consequences of the breach; and
4. the measures taken or proposed in respect of

minimising the fall out of the breach;

5. If there is a high risk to a data subject, he or she must be told.

Records must be kept of all data breaches and action taken, including those in respect of which there was no obligation to notify the regulator.

Fines – The rules in the GDPR are underpinned by a tougher penalty regime. The maximum penalty for non-compliance is EUR20 million or, if it would be higher, 4% of an undertaking's **worldwide** turnover, compared to the current maximum penalty in the UK of £500,000. Although this does not necessarily mean higher penalties in practice, this change is likely to lead to a greater focus on compliance.

10. **New European Data Protection Board** – A new advisory board will be set up called the New European Data Protection Board. The Board will be a source of opinions and guidance on the GDPR. In practice, particularly given our impending Brexit, we anticipate that our own ICO will continue in its current function and we will use this new EDPB in relation to issues arising from data transfers to the EU.

11. **Binding corporate rules** – The need for binding legal frame works governing data transfer outside of the EU is becoming more and more important, particularly with the issues concerning Safe Harbour. Multi-national controllers will be able to transfer personal data outside of the EU more easily, provided the group has stringent internal controls over how the data is treated. Such controls will take the form of Binding Corporate Rules.

What should employers do now?

DON'T PANIC!

You are probably already most of the way to achieving compliance and what the GDPR introduces is an opportunity to complete that final stage of the process. If you like, we can use different fractions of compliance, but the opportunity is still there!

Plan - the revised rules will not apply until the summer of 2018 but it is really important to start getting to grips with the incoming changes and build data protection into how your business captures data and processes it.

Steps we suggest may include:

1. consider appointing a DPO and whether appointment would be mandatory;
2. review privacy notices and other fair-processing information given to individuals and consider what additional information will need to be included;
3. review contracts and standard documents to see whether and how they deal with data protection and in particular, whether contractual "consent" is sought. If consent is obtained in a standardised way, you will need to consider setting out data protection consents in a separate schedule;
4. establish a policy (with dedicated personnel and a timeline) for handling data breaches; and
5. undertake regular impact assessments - obtain a full picture of exposure to potential data breaches by ensuring that breaches and loss are reported to whoever is responsible.

We hope that this information sheet is useful. If you are uncertain about anything compliance related, please speak to our Data Protection team.

Laura Trapnell

Head of IP
023 8048 2114
laura.trapnell@parissmith.co.uk

Crispin Dick

Partner
023 8048 2107
crispin.dick@parissmith.co.uk

Cliff Morris

Partner
023 8048 2289
cliff.morris@parissmith.co.uk

Arezou Rezai

Solicitor
023 8048 2330
arezou.rezai@parissmith.co.uk