General Data Protection Regulation:
Key provisions and what businesses should be doing now

In 1995 the internet entered public consciousness. Hitherto it had been supported by state funding but afterwards it was completely privatised, which saw internet providers like America Online offering access to the World Wide Web system for the first time.

It also saw the introduction of the Data Protection Directive, which established a regime across all EU countries.

Since then, there have been significant advances in information technology, and fundamental changes to the ways in which individuals and organisations communicate and share information.

In addition, the various EU member states took divergent approaches to implementing the Directive, creating compliance difficulties for many businesses.

For those reasons, the EU's legislative bodies, national data protection authorities and member states have spent considerable time over the last 4 years preparing an updated and more harmonised data protection law, which we will be talking about today.

The General Data Protection Regulation has already come into force but EU member states must transpose it into national law by 6 May 2018.

Please don't cling to Brexit as an excuse for avoiding compliance with the Regulation. In the words of Elizabeth Denham, the UK's Information Commissioner, "I don't think Brexit should mean Brexit when it comes to standards of data protection."

Data Protection in the news

Many of you will read about the latest travails of that bastion of the gig economy, Uber, last week. Some of you will have accounts with Uber. If so, you will be one of 57 *million* customers and drivers to have their information hacked.

Should you be concerned at the way Uber handled the problem? Well, the UK's information commissioner thinks so. Not only did Uber keep quiet about the breach, they paid a ransom to hackers to delete the data.

It is always a company's responsibility to identify when UK citizens have been affected as part of a data breach and take steps to reduce any harm to consumers. Deliberately concealing breaches from regulators and citizens could attract higher fines for companies.

It follows that, if UK were affected, the information commissioner should have been notified to enable them to assess and verify the impact on people whose data was exposed.

In practice the Information Commissioner's Officer (ICO) would work with the National Cyber Security Centre to determine the scale of the breach and how it

affected people in this country, as well considering the next steps that Uber needed to take to comply "with its data protection obligations".

Next year, EU countries will radically alter data protection laws to offer consumers greater control over the data they share with companies.

As we will see, the Regulation aims to impose huge fines on companies that conceal data breaches.

Under those rules, companies have to notify data regulators about a breach within 72 hours of becoming aware of a hack.

They face fines of 4% of their global annual turnover or 20 million euros (£18m), whichever is higher, if they are found to be in breach of the Regulation.

As Uber hasn't released its figures, we can't speculate as to the potential final cost of the fine, but it is fair to say the regulator would come down hard and under the regulations it would likely be in the tens of millions.

The greater cost to Uber however would and will be in terms of reputation, which although harder to quantify than a fine could far outstrip any penalty handed to them by a regulator.

Given the current climate around data security and breaches, it is astonishing that Uber paid off the hackers and kept this breach under wraps for a year.

The fact is there is absolutely no guarantee the hackers didn't create multiple copies of the stolen data for future extortion or to sell on further down the line.

But perhaps the key point to take from this debacle is this: If you were (or are) a customer of Uber will you feel that it has treated you with respect?

Probably not.

Millions of people will now be worrying over what has happened to their personal data over the past 12 months, and Uber is directly responsible for this.

Moreover, in opting to not only cover up the breach, but actually pay the hackers, Uber has arguably directly contributed to the growth of cybercrime and the company needs to be held accountable for this.

In essence the Regulation is designed to protect customers by giving them confidence that the businesses they buy from are looking after their personal data.

The Regulation – Key Points

Be proactive

Make sure that decision makers and key people in your organisation are aware that the law is changing. They need to appreciate the impact this is likely to have and identify areas that could cause compliance problems.

Start by looking at your organisation's risk register, if you have one.

Remember that implementing the Regulations could have significant resource implications, especially for larger and more complex organisations.

You may find compliance difficult if you leave your preparations until the last minute.

What is personal data?

Broadly speaking, personal data relates to a living individual whom the holder of the data can identify.

Now, you and I may assume that personal data implies that information is kept and processed electronically, but in fact it extends to paper and other manual records

- intended to be processed electronically; and
- contained in a relevant filing system or intended to form part of one.

It follows that an untidy pile of papers in the corner of a room may fall within the definition of a "relevant filing system" if they are waiting to be organised into one, so be warned!

Do businesses need consent before processing personal data?

There are several scenarios where it will be legitimate to process personal data without the customer's prior consent.

One is to allow "contractual performance" where

- processing is necessary for the performance of a contract to which the data subject is a party. This may include, for example, processing the address of the data subject so that goods purchased online can be delivered, or processing credit card details in order to effect payment; or if
- processing is necessary prior to entering into a contract such as pre-contractual relations (provided that steps are taken at the request of the data subject, rather than being initiated by the controller). For example, if an individual requests information from a retailer about a particular product, the processing of that individual's personal data is permitted for the purposes of responding to that enquiry.

Another is to allow processing for "legitimate interests", which will require a balancing of the legitimate interests of the business against the interests and fundamental rights of the data subject. To determine this balance, you must consider a number of factors, including:

- the nature and source of the legitimate interest;
- whether the relevant processing activity is necessary for the exercise of a fundamental right, or is otherwise in the public interest;
- the impact on the data subject;
- the data subject's reasonable expectations about the processing of his or her personal data;
- the nature of the data and how it is processed;
- whether the business can put in place additional safeguards to limit any undue impact on the data subject (e.g. data minimisation).

If, after weighing these factors, it is clear that the processing causes undue interference with the interests, rights, or freedoms of the affected data subjects, you really should not claim that data is being processed legitimately.

Data can also be processed to protect an individual's "vital interests". This condition only applies in cases of life or death, such as where an individual's medical history is disclosed to a hospital's A&E department treating them after a serious road accident.

Finally, businesses may process personal data where the controller has a legal obligation to perform such processing. A "legal obligation" in this context means a legal obligation arising under EU law or the laws of a Member State. A legal obligation to process personal data arising under the laws of a non-EU jurisdiction (e.g. an obligation arising under US law) does not provide a lawful basis for processing personal data, nor does responding to a request from HMRC by providing information if doing so is not legally mandatory.

Any processing which falls outside the Regulation will require the business to demonstrate that the data subject gave their consent to the processing and it will be the business that bears the brunt of proving that consent was validly obtained.

When the processing has multiple purposes, the data subject should give their consent to each of the processing purposes.

The data subject shall have the right to withdraw their consent at any time. It must be as easy to withdraw consent as to give it.

It follows that businesses that rely on consent, as a legal basis for processing personal data, will need to carefully review their existing practices to ensure that any consent they obtain indicates affirmative agreement from the data subject (opt in) (for example, ticking a blank box). Mere acquiescence (for example, failing to un-tick a pre-ticked box) does not constitute valid consent under the Regulations.

Another important point to be aware of is this: businesses cannot rely on consent as a legal basis for processing if there is a "clear imbalance" between the parties. This

imbalance may be evident in the relationship between the employer and employee as consent is presumed not to be freely given.

In summary, then, the Regulation makes it much more important to engage with and to demonstrate the grounds for lawful processing of personal data you seek to reply on. In particular it will be much harder to rely on individuals' consent as a valid reason to hold and process their personal data. If consent is the basis on which a business seeks to justify the lawful processing of personal data, that consent will have to have been informed, freely given, specific and unambiguously shown. This means that a pre-ticked box on an online consent form or the inclusion of a short, generic acknowledgement in an employment contract will not suffice.

Protect personal data

The Regulation lays down rules relating to the protection of individuals with regard to the processing of personal data.

They are intended to protect the fundamental rights and freedoms of individuals and in particular their right to the protection of their personal data.

The Regulation describes personal data as

> "…. any information relating to an identified or identifiable person, i.e. someone who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

Personal data should only be

- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date; and
- retained in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

The watchwords are:

- lawfulness, fairness and transparency
- purpose limitation
- data minimization
- accuracy

- storage limitation
- integrity and confidentiality

You must accordingly document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit across the organisation or within particular business areas.

The Regulation requires you to maintain records of your processing activities. It updates rights for a networked world. For example, if you have inaccurate personal data and have shared this with another organisation, you will have to tell the other organisation about the inaccuracy so it can correct its own records. You won't be able to do this unless you know what personal data you hold, where it came from and who you share it with. You should document this. Doing so will also help you to comply with the accountability principle, which requires organisations to be able to show how they comply with the data protection principles, for example by having effective policies and procedures in place.

Basic security consideration

One of the requirements of the Regulation is that, by using appropriate technical and organisational measures, personal data shall be processed in a manner to ensure the appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

What is a personal data breach?

According to the Regulation:-

> "…. breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed

What is meant by "destruction" of personal data should be quite clear: this is where the data no longer exists, or no longer exists in a form that is of any use.

"Damage" should also be relatively clear: this is where personal data has been altered, corrupted, or is no longer complete.

In terms of "loss" of personal data, this should be interpreted as the data may still exist, but the business has lost control or access to it, or no longer has it in its possession.

An example of loss of personal data can include where a device containing a copy of a customer database has been lost or stolen. A further example may be where the only copy of a set of personal data has been encrypted by ransomware, or has been encrypted by someone in your organisation using a key that is no longer in your possession.

Finally, unauthorised or unlawful processing may include disclosure of personal data to (or access by) recipients who are not authorised to receive (or access) the data, or any other form of processing which violates the Regulations.

What if data is temporarily unavailable?

According to an EU Working Party, this may be a personal data breach. It could happen if there has been significant disruption to the normal service of an organisation, for example, experiencing a power failure or denial of service attack

In the context of a hospital, if critical medical data about patients is unavailable, even temporarily, this could present a risk to individuals' rights and freedoms; for example, operations may be cancelled.

Conversely, in the case of a media company's systems being unavailable for several hours (e.g. due to a power outage), which prevents it from sending newsletters to its subscribers; this is unlikely to present a risk to an individual's rights and freedoms.

Personal data breach

The consequences of a personal data breach can potentially have a range of significant adverse effects on individuals, which can result in physical, material, or non-material damage. The Regulation explains that this can include (amongst other things) loss of control over their personal data, identity theft or fraud, financial loss, damage to reputation and loss of confidentiality of personal data protected by professional secrecy.

Notification

As a result, the Regulation requires the breach to be notified to the office of the Information Commissioner, unless it is unlikely to result in a risk of such adverse effects taking place. Where there is a likely high risk of these adverse effects occurring, the Regulation also requires the business to communicate the breach to the affected individuals as soon as is reasonably feasible.

It will be mandatory to record all personal data breaches and, additionally, to report breaches to the supervisory authority unless there is unlikely to be a risk to the rights and freedoms of individuals. High-risk breaches will also need to be reported to the affected individuals (subject to some exceptions).

An EU Working Party has proposed guidelines on the data breach rules, including on how to approach the risk assessment and determine whether a breach needs to be reported, and when and how breaches should be notified and documented.

In terms of the risk assessment, the guidelines state that businesses will need to consider factors such as the nature, sensitivity and volume of personal data and the severity of the consequences for the individuals - for example, where the breach involves special categories of personal data such as data about health or sex life or

personal data about vulnerable individuals, the potential damage to individuals could be particularly severe and there may be more risk.

Remember that personal data breaches do not necessarily have to be cyber-attacks and can take various forms, including confidentiality breaches (unauthorised disclosures of personal data), availability breaches (the unauthorised or accidental loss or destruction of personal data) and integrity breaches (the unauthorised or accidental alteration of personal data).

One of the key points in the guidelines is around the timing of notifying breaches to the ICO. This should be done without undue delay and, where feasible, within 72 hours of the business having become "aware" of the breach. According to the guidelines, a business should be considered to be *aware* when it has "*a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised*". In the case of a loss of a CD with unencrypted data this will be when it realises the CD has been lost. However, crucially, where the business uses a processor to process personal data on its behalf, the Working Party considers it will be aware when the processor has become aware (whether or not the processor has actually notified the business concerned).

Here, and in order to cover your backs, you may therefore wish to impose additional contractual obligations on their processors to flag breaches promptly, potentially with a short backstop, to enable them to review and report breaches in time.

To help businesses comply with their obligations, I suggest having a documented notification procedure, setting out the process to follow once a breach has been detected, including how to contain, manage and recover the incident, as well as assessing risk and notifying the breach. Delaying notifying a breach or failing to document a breach could lead to fines or other enforcement action.

<u>Data subject access requests</u>

At present, individuals who want to see a copy of the information an organisation holds about them can make a subject access request. Upon payment of a fee, they are entitles to ne told

- told whether any personal data is being processed;
- given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people; and
- given a copy of the information comprising the data; and given details of the source of the data (where this is available).

An individual can also request information about the reasoning behind any automated decisions, such as a computer-generated decision to grant or deny credit, or an assessment of performance at work.

In most cases you must respond to a subject access request promptly and in any event within 40 calendar days of receiving it.

The Regulation now requires you to respond to a SAR within one month from the date of receipt of the request and provide more information than was the case previously.

As a result, businesses should plan how they will respond to data subject access requests within the new time scale and how they will provide the additional information required.

If your organisation handles a large number of access requests, consider the logistical implications of having to deal with requests more quickly. It may be feasible or desirable to develop systems that allow individuals to access their information easily online.

The right to erasure

The Regulation allows individuals to ask that businesses delete their personal data in certain circumstances (for example, if the data is no longer necessary for the purpose for which they were collected or the data subject withdraws their consent).

Whilst it remains unclear precisely how this will work in practice. businesses will need to devote additional time and resources to ensuring that these issues are appropriately addressed.

In particular, businesses should consider how they will give effect to the right to erasure (right to be forgotten), as deletion of personal data is not always straightforward.

Privacy by design

Privacy by design is an approach to projects that promotes privacy and data protection compliance from the start. The idea is to make sure that at the early stages of any project, and then throughout its lifecycle, businesses integrate core privacy considerations when (for example):

- building new IT systems for storing or accessing personal data;
- embarking on a data sharing initiative; or
- using data for new purposes.

Taking a privacy by design approach is an essential tool in minimising privacy risks and building trust. Designing projects, processes, products or systems with privacy in mind at the outset can lead to benefits which include:

- Potential problems are identified at an early stage, when addressing them will often be simpler and less costly.

- Increased awareness of privacy and data protection across an organisation.

- Organisations are more likely to meet their legal obligations

- Actions are less likely to be privacy intrusive and have a negative impact on individuals.

The Regulation will expect businesses to be able to demonstrate that, when building from the ground upwards, the impact on individuals has been considered and taken into account.

Conclusion

This note cannot provide a comprehensive statement of all that your business should do to prepare for and to be compliant with the GDPR - and it is important to dedicate personnel and resources to fully understand how the new rules will affect your own business and to plan accordingly. However as a minimum, your business should at least consider taking the following steps now, in preparation for the new regime:

- Decide who will be responsible for understanding and engaging with the implications of the GDPR within your business and ensure that they have the time and resources to dedicate to doing so, including expert external support and buy-in at a senior level.

- Audit current data protection practices and documents such as website privacy policies for potential areas of non-compliance. Pay particular attention to the following questions: How is the data gathered? What are individuals told about how the data is to be used, and how does that match with reality? What is the data used for? Who has access to the data? To whom is the data disclosed and why?

- Consider the purposes for which you may wish to gather and use customers or clients' personal data, and then review all related documents, policies, practices and training to ensure that they are fit for purpose.

- In the employment context, consider the purposes for which you may wish to use employees' personal data and then review all of your current employment documents, policies and recruitment & HR practices and adjust them to ensure that they are adequate.

- In each case, think carefully about the grounds for lawful processing that you will seek to rely on. If you are relying on 'consent', ensure that you can demonstrate all that the new regime requires in order for consent to be valid.

- Consider internal policies and systems to help deal with the new governance obligations, including individuals' new rights and the new obligation to report breaches.

- Check contracts with suppliers such as payroll providers and IT consultants, where they might process personal data on your business's behalf. Those contracts must contain clauses which deal specifically with personal data, limiting its use. Contracts should also contain an obligation on the supplier to inform the client immediately of any breach of security or loss or damage to the personal data.

Remember the importance of accountability - identify not only what you will do but also how you will 'demonstrate compliance'.

Paul Gardner

paul.gardner@gardnerthorpe.co.uk

Gardner Thorpe
72 High Street
Haslemere
Surrey
GU27 2LA

01428 661151