What is GDPR?

Martin Hynes - Commercial Director

After attending many networking meetings recently and briefly bringing the topic of GDPR into conversation I was surprised that so few people had heard anything about GDPR. When I say few, I mean none. Most people either didn't believe it was going to come into force or perhaps thought that in fact was not going to impact their company at all.

What will you get from reading this ebook?

I have tried to give a general overview of what GDPR is and how it could impact you and your business in one read with the aim of getting you to put this on your agenda as a priority before it's too late.

What does GDPR stand for?

GDPR stands for General Data Protection Regulation so yes, this is about data and more specifically personal and private data.

What is GDPR?

GDPR is a new regulation that is coming into force in 2018 that will impact the way you think about and handle customer data in your business. It is designed to ensure that all personal and customer data is handled and managed in a way that gives individuals the right to choose how the data is collected, stored and processed.

What is GDPR?

When does this start in the UK?

It comes into play in the UK on 25th May 2018 and the UK's commitment to leaving the EU has no impact on this date or the regulation.

Who does this impact?
Everyone who holds data about their clients and customers. This is not just about big companies and there is no sliding scale of when you need to be compliant. The data and the standards are the same regardless of the size of your company.

What kind of Data are we talking about?

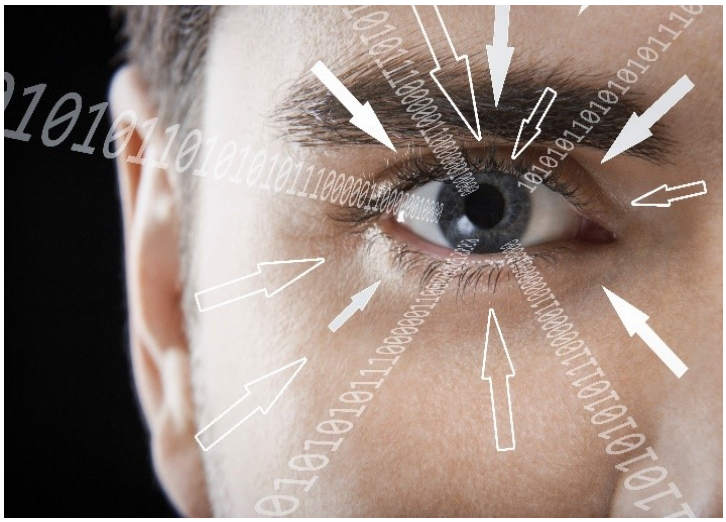
As mentioned above, GDPR is about personal and private data. This is the same as the Data Protection ACT, but GDPR's definition is far more detailed and inclusive.

This is due to how technology has evolved and how information such as a customer's IP address is considered personal data.

Almost all companies keep records such as HR, Customer Lists and contact details. All of this is data that falls under GDPR.

Think of it this way, any data that could identify an individual need to be considered.

What is GDPR?



Controllers and Processors

GDPR applies to both "Controllers" and "Processors"; but what do these terms mean?

Definition of a controller is "*means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data*"

Definition of a Processor is "*means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller*"

The term "processing" is very broad. It essentially means anything that is done to, or with, personal data (including simply collecting, storing or deleting that data). This definition is significant because it clarifies the fact that EU data protection law is likely to apply wherever an organisation does anything that involves or affects personal data

The main difference of note here is that in the current data protection act, only the controller was liable for the data and any breaches. Whereas now both controllers and processors are both liable.

What is GDPR?

If your business falls into the data processor category then you must be able to demonstrate how you document and ensure the following:

- Name and details of your organisation (and where applicable, of other controllers, your representative and data protection officer).
- Purposes of the processing.
- Description of the categories of individuals and categories of personal data.
- Categories of recipients of personal data.
- Details of transfers to third parties, including documentation of the transfer mechanism safeguards in place.
- Retention schedules.
- Description of technical and organisational security measures.

You may be required to make these records available to the relevant supervisory authority for purposes of an investigation.

For many companies, you may in fact be both a controller and a processor.

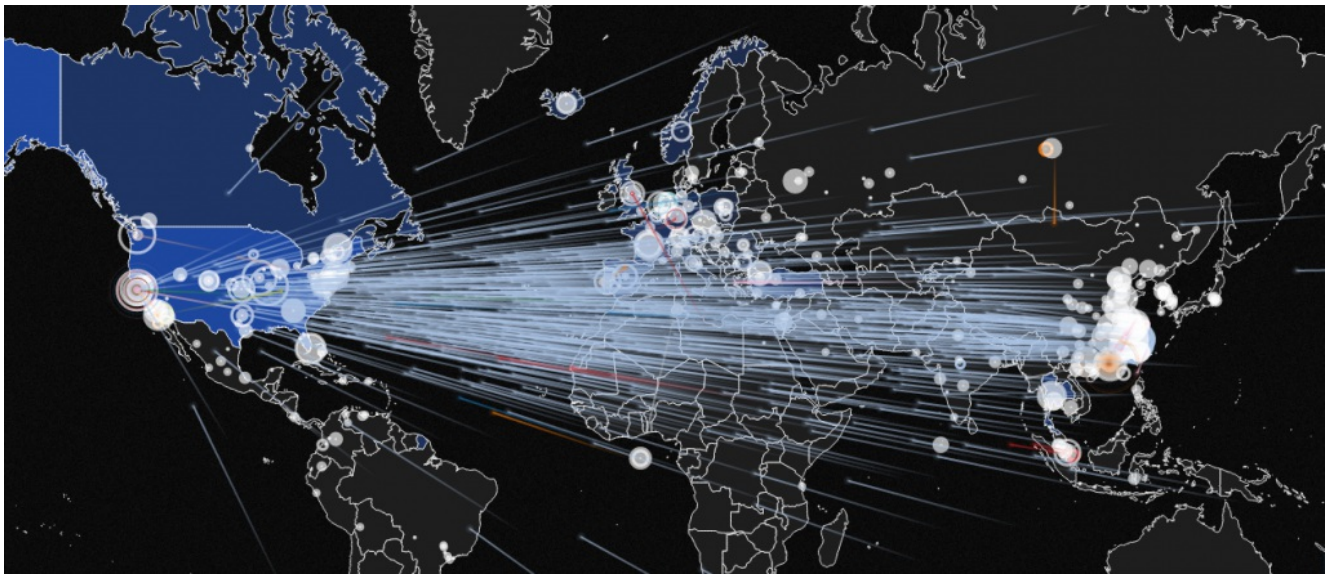
What do you need to do now?

First, I highly recommend just ensuring that all the key stakeholders in your company are aware that the law is changing and that they need to understand what this means to their company.

Start documenting what personal information you hold, where It came from and who you share it with.

Check your procedures and make sure they cover what rights people have over their personal data and how and when it is deleted and the procedure for those that request a copy of their data (more on this later).

Check, and if needed, update your procedures for how you obtain consent when collecting personal data. Also, if you collect data on anyone aged under 16, do you have consent from their parents or guardians?



Data breaches

This is the area that most people think GDPR is all about. Yes, data breaches are a part of it, but its more how you stop the breaches happening in the first instance and what you need to do if one were to occur.

As I am sure you have heard in the news over the last few years there have been some very high-profile cases where customers have had their systems hacked and tens of thousands of customer records containing sensitive data including credit card and bank details have been stolen.

We heard about these as they are high profile. What about all the breaches that happen year after year at smaller companies?

In most cases there was lots of opportunity to prevent these breaches and it comes down to a lack of policies and procedures and sometimes lack of investment in the right security systems.

So, what happens if you are breached?

Regardless if GDPR has come into play or not, you need to report it. Once it is in play not reporting it has significant consequences.

The type of data that has been breached determines who is notified. In all cases the relevant authorities are notified and in some cases the people affected are also notified.

A notifiable breach must be reported to the relevant supervisory authority within 72 hours of the organisation becoming aware of it.

If the breach is sufficiently serious to warrant notification to the public, the organisation responsible must do so without undue delay.

Failing to notify a breach when required to do so can result in a significant fine. The fines are in fact based on a two tier system depending on the severity of the breach. For the more serious breaches the fine could be up 20 million Euros or 4% of the company turnover whichever is higher and the 2nd tier is up to 10 million Euros or 2 per cent of your global turnover .

The higher of those fines are likely to be for those companies that really should know better and where personal data is a huge component of their business. Think banks, credit card companies, mobile phone network providers and other similar public services where personal data loss could mean serious financial and intrusive affects for those whose personal data has been exposed.

To give you some context the previous maximum penalty for a similar breach would have been £500k.

What is considered a breach of personal data?

Anytime that an individual's data is comprised by someone who was not intended to have access to that data. This includes:

- Destruction of data
- Loss of data
- Alteration of data
- Unauthorised disclosure
- Or simply unauthorised access

This shows that a breach is far more than just loss of data.

How to prepare to report potential breaches?

To comply you must have a very clear procedure in place that outlines exactly how to identify and report a potential breach of data. Your staff should understand what is a potential breach and exactly what the procedure is for reporting one.

The rights of individuals

GDPR states that individuals have the right to control what companies can and cannot do with the data they hold about them. These rights are as follows:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

Individuals can make requests to any company they believe holds personal information about them and make these requests listed above. To comply with GDPR you must have procedures for each of them.

The right to erasure is also known as the “the right to be forgotten”. This means that if you receive such a request you must ensure that not only do you delete the data that you hold, but also ensure any third parties also delete data that you have passed on to them.

Rights in relation to automated decision making and profiling is where any computerised system could decide based on data and a set of automated rules. Individuals have the right to insist on human intervention to express their point of view and or obtain an explanation of the decision and the ability to challenge it.

Now this only applies when the automated decision produces a legal effect or similar significant effect on the individual.

How long do you have to respond to these requests?

How long you have to respond depends on how you obtained the data about the individual.

If you gained the data straight from the individual then you must respond to that request straight away.

If you obtained the data from a source other than direct from the individual you are expected to respond in a reasonable time frame which is suggested to be no more than a month from when you first received the request.

How do you manage all of this?

The GDPR requires that privacy is included in systems and processes by design.

What does this mean to a small business owner? It means that you need to be able to demonstrate that any new technologies introduced to the business are checked for how they handle and manage privacy.

It also means working closer with your IT department or provider to ensure that where data is collected, by default, privacy is set and does not require manual intervention from the individual to ensure their private data is kept private.

You also need to ensure that personal data is not by default accessible to all but in fact only available to those that absolutely need it.

Appointment of a Data Protection Officer

GDPR states that the appointment of a Data Protection Officer (DPO) is mandatory for the following:

- All public authorities
- Any company or any size that processes lots of personal information of individuals on a regular or systemic basis.

The role of the data protection officer can be provided by either an employee or even by a third party service provider.

What is GDPR?

How is IT impacted by GDPR?

There is a reason that IT companies such as ourselves are informing and educating about GDPR. Having the right security stack in place alongside the documenting of the processes will go a long way to achieving compliance.

Being able to demonstrate how you protect and backup your data in the first place will be required in any potential investigation.

Also ensuring you have invested in the right services, systems and training to minimise any potential breaches is essential as you will be expected to be able to demonstrate exactly where and how all of your data is stored and processed and in the event of a breach be able to show how and where your systems failed.

Leaving any one of these out will mean you have a huge hole in your IT security and therefore are not compliant to GDPR and open to potential breaches and subsequent fines.

Getting your staff trained on the very real dangers of cybersecurity is one huge step in the right direction and demonstrates that you are taking the steps to ensure your staff are aware of the different dangers, how to spot them and what to do about them. BCS have produced an online training course that will make sure you have this covered whilst at the same time providing vital training for your staff. This can be found at www.bcseducation.co.uk . Not a customer of BCS? No problem, simply attend one of our Cybersecurity lunch and learns where all attendees get access to the online training for you and all your staff. To book into the next session simply click here.

Just our way of doing what we can to educate as many people as we can and support the Kent Community.

What is GDPR?

Summary

GDPR affects business of all sizes and really is an opportunity. This enables companies of all sizes to get a grip of data protection and privacy and put the procedures and technology in place to not only meet compliance purposes but also gain peace of mind. This does not need to be expensive and in many cases, these are services or procedures you just never got around to putting in place.

Overwhelmed?

Don't be, although this all sounds like a lot to process (no pun intended) BCS are here to help you every step of the way. We may not be experts in GDPR but we do understand what you need to do from an IT perspective to be safe, secure and compliant.

Our Managed Services stack includes all the services and technology required to ensure our clients are safe and secure, a big PLUS when aiming for compliance. As technology evolves, so does our stack.

Want to learn more?

Check out our Lunch and Learn events where we cover both Cybersecurity and GDPR. These events get booked up very early so get yourself booked in here.

Should you wish to discuss any of the above I would be more than happy to help you get a better understanding of how GDPR impacts both your business and your IT and help you get ready for May 2018.

You can email directly on martin.hynes@bcs365.co.uk