The General Data Protection Regulation [Q&A]

Q. Will it affect your business after Brexit?

The simple answer is yes. Article 50 might not be triggered by the time this law comes into force which means we will still be covered under it. The Data Protection Act will also be amended to reflect the General Data Protection Regulation.

Q. Would your IT Provider be able to be the Data Protection Officer?

No, the data protection officer needs to be someone within your organisation. However your IT Provider can help appoint one and give knowledge on what they need to know.

Q. Are Directors personable liable for this legislation?

According to the Information Commissioner's Office, the new accountability principle requires you to demonstrate that you comply with what is outlined in the regulation and states explicitly that it is the responsibility of the Directors.

Q. If you follow all the rules but still have a breach, will you still be fined?

If you have got the policies in place and taken all the reasonable steps to mitigate the risk then it is unlikely that you will be fined.

Q. If I receive an email from someone with their phone number on – Is that data under this law?

If the information (name, email, phone number) is open to the public, such as on a website or in an email signature, it might not be classed as a breach as this isn't information that needs to be kept secure.

Q. How does the GDPR compare to other parts of the world?

At the moment Switzerland and Germany are at the top. The UK are behind on this law as it was first set up before mobile phones and data on the internet took over the way we work. This new legislation will improve the way Europe deals with Data.

Q. What if there is a breach in the U.S that affects my data? Am I still liable?

This will depend on the measure you put in place before you sent your data and how the breach occurred. There is a section of the regulation which places restrictions on the transfer of personal data outside of countries and international organisations, with less control and levels of protection than those covered by the General Data Protection Regulation. Encrypting your data is one measure that can be put in place to avoid a data breach.

Q. Are there separate rules or guidelines on paper documents and data that is sent in the post?

The GDPR does not just affect digital data: the text doesn't mention any carrier or data formats at all. This means that physical data containing data and personal data in any physical format is included as well. This includes documents such as payslips, contracts, HR forms and anything with secure personal information on.

Q. Are charities and voluntary groups affected?

Charities and voluntary groups are affected by the GDPR. The legislation has put a big emphasis on the need to comply as a data processor and a data controller, which means that charities themselves who deal with data need to ensure it is protected as well as if they are using the services of a supplier to collect and store their data.

Q. Does this apply to Governments?

The GDPR applies to all companies and organisations that process personal data of European citizens, no matter what size they are or the industry they are in. As the Government don't have a global turnover, they will probably just be hit with a big fine.

Q. Is there a definition of personal data?

In article 4 it states "*'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular 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".*

Q. If you encrypt everything, how does everyone see it?

Encryption works by converting data into a specific code which can then be viewed by someone with an encryption key. Even if someone gets access to your data, that can't read it or do anything with it without the key. Data at rest and movement of data both need to be encrypted and there is software that can help you do this.

Q. With things like the Office 365 platform where everything is a single login, how can we be sure we are protected?

Having processes and policies in place such as Identity and Access Management and multifactor identification will make it harder for criminals to gain access.

Q. If I have all my data in the Cloud – would I still be responsible or would it be the Cloud provider?

Under the GDPR both your business 'the controller' and your Cloud provider 'the processor' will be responsible.

If you are a processor, the GDPR places specific legal obligations on you; for example, you are required to maintain records of personal data and processing activities. You will have significantly more legal liability if you are responsible for a breach. These obligations for processors are a new requirement under the GDPR.

However, if you are a controller, you are not relieved of your obligations where a processor is involved – the GDPR places further obligations on you to ensure your contracts with processors comply with the GDPR.

Q. Is this going to fall under ISO?

If you have things like ISO 9001 or 2701 then it will overlap with some of the scope of the GDPR so you are further ahead than most businesses who haven't even thought about it.

Q. Is there a percentage of how many times an IP address is breached compared to how many times you know about it?

The answer to this question will vary significantly from business to business. The amount of times a breach occurs will depend on what security software you have in place and how many times you detect it will also depend on if you have software to even detect and report on it. There is software that you can use to detect and protect against data breaches which we can discuss with you.

Q. It's not just about the technology we have to put in place, surely we have to change the mentality of our staff too?

This is exactly right. The majority of breaches or cyber-attacks occur because of internal staff, not necessarily through malicious behaviour but through their lack of awareness of online threats. We can provide Cyber Awareness Training for your staff to ensure they have best practices in place to avoid being hit by online attacks.

The topic of GDPR is enormous and will grow momentum as we draw closer to 25th May 2018. As new recommendations crop up and people provide their interpretation of the legislation, there will be many more questions. If you have any other questions that aren't covered in this document or you would like to discuss this further, we can help to advise and make sure you are prepared.

www.metaphor-it.com | 03330 033305 | info@metaphor-it.co.uk

Head Office: The Baltic Exchange, 38 St Mary Axe, London, EC3A 8BH
Operations Centre: 7, Perrywood Business Park, Honeycrock Lane, Redhill, RH1 5DZ