Digital Interruption

Getting to the Point of GDPR

what you really need to know to

prepare for the new regulations

+44 (0)161-820-3056
www.digitalinterruption.com
contact@digitalinterruption.com

How GDPR will affect your business

As security consultants who specialise in project management, policy and data protection regulation (along with testing and training), we are getting a lot of questions about GDPR. There seems to be some uncertainty as to what it is, doubt about who it will affect and if it will even go ahead in the light of Brexit. With numbers such as €20m Euros hitting the headlines when it comes to fines, there is understandably some sense of fear.

But is GDPR really all that daunting and what exactly is it? Well, we can help you there.

GDPR stands for General Data Protection Regulations. It is a new set of regulations, set by the European Parliament, with the intention of unifying data protection for all individuals across the European Union and strengthening those individuals rights when it comes to their personal data. The idea is to give the individual control of the data that is kept about them.

The regulation was adopted on 27 April 2016 and will become fully enforceable on 25 May 2018, and yes, as the UK is currently still part of the EU it applies to all organisations in the UK that hold personal data, regardless of their size.

GDPR is not just about security testing. It's about how you use and secure data, so here is a quick guide to help you with some of the points you as an organisation will need to consider.

DIGITAL INTERRUPTION

Don't be afraid of change, change is good

Yes, there is going to be more red tape, but this doesn't have to be a headache for your organisation. In reality under the current Data Protection Act (DPA) you should already be following much of the best practice covered by GDPR. The difference is now there are greater powers of for enforcement.

The main differences (listed on the pages below) will make the data you hold more relevant and up to date and therefore more useful to you. GDPR will provide you with a framework to protect that data and by stopping it from falling in to the hands of attackers you will be protecting both your customers and your reputation.

A 2014 study by Semafone found that of a survey of 2,000 participants, people stated that they were "not at all likely" or "not very likely" to do business with an organisation which had suffered breaches involving the following types of personal data:

Credit/debit card - 86%
Home address - 83%
Telephone number - 80%
Email address - 76%

DIGITAL INTERRUPTION

If you think it applies to you, it probably does

If the DPA applies to you so does GDPR. This means if you hold personal data you must be compliant. Personal data is any information related to a natural person or 'Data Subject', that can be used to directly or indirectly identify the person. It can be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information or even an IP address.

Some parts of the GDPR will have more of an impact on some organisations than on others, for example, the provisions relating to profiling or children's data.

GDPR applies to all companies dealing with EU customers. This means GDPR needs to be enforced by those that not only have a presence in an EU member state, but also any companies that deals with EU customers even if they are based outside the EU.

Companies that rely on third parties to process data are still obliged to comply with GDPR.

Third parties can be a significant risk for data security and regulatory compliance. You will need to ensure that both your organisation and your third parties have the policies, processes in place to support your GDPR requirements.

According to the 2013 Trustwave Global Security Report on 450 global data breach investigations, 63% were linked to a third-party component of IT system administration

DIGITAL INTERRUPTION

You don't own the data, they do

The current data protection act gives individuals rights to their data, but this is extended under GDPR and is far more explicit. Consent and the right to erasure, also known as 'the right to be forgotten', are key to this.

Under the new requirements consent to the collection and use of data must be explicit, not implicit. This includes all data, even data collected before GDPR comes in to effect and you must be able to demonstrate this consent. It's worth noting not everyone wants to be contacted for marketing purposes.

Although the right to erasure does not provide an absolute 'right to be forgotten', individuals have a right to have personal data erased and to prevent processing in specific circumstances. You need to understand what these circumstances are and if they are relevant to your organisation.

Further to this individuals can ask to obtain confirmation that data is being processed, ask for access to personal data or other supplementary information, so get ready for the subject access requests. These will be similar to the existing DPA subject access request, however the information must now be provided for free and within one month of receipt.

"Many companies use email to promote themselves, but we don't want to take this approach – which many consider intrusive. Our database of customers' email addresses, including yours, will be deleted" John Hutson, Chief executive J.D. Wetherspoons

DIGITAL INTERRUPTION

It's all about the audit trail

You don't just need to protect data, you need to be able to show that you are. A lot of security consultancies will offer you a pen test, and although this can be useful it will only tell you where you are now and will only be useful if you can do something with the results.

Before considering a pen test, first think about your current security policies and procedures. This is what the regulators will want to see and for good reason.

Depending on your size and the data you hold you will need to provide clear privacy polices, follow those policies and keep internal records of your processing activities.

If you have more than 250 employees you may need to appoint a data protection officer, implement measures that meet the principles of privacy by design and data protection by default, carry out training and hold internal audits of processing activities.

Smaller organisations and sole traders will still need to maintain relevant documentation on processing activities, but other measures will depend on the data you hold. As the current regulator, the ICO will be able to advise.

ICO data shows that in the first quarter of 2016, 448 incidents of data breach or loss were recorded. Of the 448 incidents, there were 39 cases of data breaches stemming from insecure websites, which includes incidents of hacking. The remaining 409 were attributed to human error

DIGITAL INTERRUPTION

Don't try to cover your tracks

Get to know your regulators, they are not trying to trip you up. They want to help and will offer relevant guidance on what you need to do.

Some organisations are already required to notify the ICO (and possibly some other bodies) when they suffer a personal data breach. The GDPR introduces a duty on all organisations to report certain types of data breach to the ICO, and in some cases, to individuals.

If you do have a breach you need to report it within 72 hours. If it's a serious breach it needs to be as soon as possible. You should have an internal breach reporting procedure in place which should explain who to report the breach to and what a breach report should look like.

This is where your audit trail comes in. If you can show you took reasonable measures to protect the data you hold this will strengthen your case.

In light of the tight timescales for reporting it is important to have robust breach detection, investigation and internal reporting procedures. Failing to notify a breach when required to do so can result in a significant fine, so if in doubt speak up.

If you handle personal information, you may need to register as a data controller with the ICO. Registration is a statutory requirement and every organisation that processes personal information must register with the ICO, unless they are exempt. Failure to register is a criminal offence

DIGITAL INTERRUPTION

It's more than just fines

One of the main differences between the current DPA and GDPR is enforcement. This means that regulators will have the support of the law behind them to enforce compliance of the new regulations. It's not all about the fines, however the ICO have made it clear this is a power they're not afraid to use.

It's true that you could be fined, and it's true that the maximum fine could be €20m or 4% of total global annual turnover (whichever is the higher), but this relates to specific infringements. There is a lower maximum fine of €10m or 2% of total global annual turnover (whichever is the higher), again this relates to specific infringements and covers failure to notify a breach.

What is clear is fines should be 'effective, proportionate and dissuasive'. Again, the regulators are not there to trip you up, if you follow the guidance and embed data protection in to your practices a fine is unlikely.

Other enforcement could include issuing warnings of non-compliance, carrying out audits, specific remediation within a clear time frame or ordering you to delete data.

"If a business can't show that good data protection is a cornerstone of their practices, they're leaving themselves open to a fine or other enforcement action that could damage bank balance or business reputation"
Elizabeth Denham, Information Commissioner

DIGITAL INTERRUPTION

It’s never to early to start thinking about GDPR

Implementing GDPR could have significant resource implications, especially for larger and more complex organisations. With the enforcement deadline of 25 May 2018 looming, don't leave preparations to the last minute.

For more information on how Digital Interruption can help you prepare for GDPR email us at:
contact@digitalinterruption.com
or call:
+44 (0)161-820-3056

DIGITAL INTERRUPTION