THE EU GENERAL DATA PROTECTION REGULATION (GDPR)

So much to do, so little time to do it in

"Procrastination is suicide on an instalment plan"

William James

12th September 2016

The GDPR is not a nice to have. Nor is it a contractual requirement imposed to filter out the bidding process. It is a legal necessity.

Making InfoSec Part of the Culture

INTRODUCTION

The GDPR is an EU law that will come into force on 25th May, 2018. It is a very wide ranging law and will force seismic changes on governance, processes and procedures for all companies that handle data relating to any EU citizen or entity.

The GDPR is a conglomeration of current EU members' data protection laws. As such, it reaches into areas which UK law has previously not ventured. For this reason, it is essential that companies do not make the mistake that because they are compliant with the UK Data Protection Act, they will automatically be compliant with the GDPR.

The law is not only about data protection. It also addresses other 'data' issues such as privacy, defines ownership of data and regulates capture, storage, use and the rights of an individual's control over their own data. The 'right to be forgotten' and the 'right of review' are also covered by this law. Access requests have the potential to become a major cost centre for all companies.

National regulators will police the GDPR. They are being given sharp teeth to achieve this and non-compliance will not be a sensible option. Whilst the vigour of individual national regulators may vary, the European Commission will be keen to see that the law is applied equally across borders. Some jurisdictional arbitrage – where a business will endeavour to be dealt with by a less aggressive regulator - may occur, but this is likely to be a dangerous and potentially costly tactic. Where a data breach involves a subsidiary of a larger company, regulators are indicating that fines will be based on the global revenue of the whole entity, not just the the subsidiary. Punishment for non-compliance will be up to 4% of annual global turnover, with an initial cap of €20m. We expect this to rise once regulators get a taste for the revenue. The law applies to non-EU companies that process or store the data of EU citizens or EU companies.

Whilst the implementation of this law is still some months away, preparation needs to begin now. Companies will need to know – that is know, not, have a ballpark understanding of - what data they hold, where it is and what they are doing with it. This likely creates a major logistical headache for most businesses. Few could conduct this exercise right now with any confidence of accuracy. Enterprises will often need to trawl across multiple platforms in order to establish their true data footprint – and then they will still need to be able to extract it and present it on demand. Third Party involvement in the processing or storage of data potentially exponentially raises the difficulty of this data discovery exercise. This task will be complex and probably a challenge, particularly where a Third Party vendor resides and/or operates outside of the EU.

General awareness of the GDPR, and the impact it is going to have, is very low. This must change soon so that the necessary preparation can be conducted. If companies attempt to park the compliance of the GDPR within the IT Department, there is a serious risk that the consequences of such a move will prove devastating. The GDPR impacts ALL areas of business;

marketing, sales, HR, etc., not just IT. We also need to understand that the Internet of Things (IoT) is already changing our risk environment. Wearables, mobile devices and removable media will all need to be factored into the discovery process in order to measure your exact data exposure. The Board and C-Suite must actively manage compliance with the GDPR and be compliant in good time. It should be assumed that regulators may seek to put an early miscreant in the public 'stocks', *pour encourager les autres*. Let's make sure that you are not that company.

AWARENESS

So far, this law has been poorly promulgated. Anecdotally, awareness is patchy at best, abysmal at worst, with smaller companies largely blissfully ignorant of the tsunami heading toward them.

'Brexit' has muddied the water. We should have some concern that enterprises may wrongly assume that the 'Leave' vote means that UK companies will not be subject to the GDPR. This is wrong, and dangerous complacency. The UK DPA, the Office of the Information Commissioner, has made it clear that the UK will adopt the law and her office will enforce it - but even if this decision is subsequently varied, any company that seeks to do any form of business in the EU or with EU entities or citizens will need to be compliant with the GDPR.

Few businesses could easily withstand a fine at the top end of the GDPR penalty scale. Half say that a fine of 4% of annual turnover will have a significant impact on their business – probably requiring the purchase of condolence cards. In addition, business will have to contend with the unavoidable, potentially very high, cost of mitigation and compensation following a breach.

Data Protection budgets have traditionally been defined by the difficulty of accessing sufficient resourcing. The GDPR has Boards and executives firmly in its sights. It is deliberately intended to force companies to adequately care for data in its care. Huge fines, public approbation and personal jeopardy for individual executives will be waiting for any company which fails to comply with the GDPR. Compulsory disclosure of data breaches (within 72 hours) added to the general demeanour of regulators to create examples of those who chose to be non-compliant will ensure that swift action will be taken against those who fail to achieve required standards. It is estimated that as many as 95% of all data breaches have their genesis in user error (which will be defined by the regulator as a failure of governance and therefore negligence) or insider malicious acts by employees or contractors (which will also likely be defined by the regulator as a failure of governance and therefore negligence), it will be critical that executives keep a firm hand on the Information Security 'tiller' and failure to do so will result in individual executives being targeted by the regulator.

Usually, due to their lack of scale and deep pockets, SMEs are the most vulnerable to cyber attack and data breach. They are often easy targets; management is not engaged, defensive sophistication is lower, technical defences will be out of their financial reach and training budgets are frequently non-existent. Yet it is a fact that simple InfoSec hygiene, which is within the reach of every company, massively reduces the chances of an SME becoming a target and therefore a victim. SME's are the source of perhaps 4 in 5 breaches in larger companies – where the criminal uses the SME as a stepping stone to the ultimate target. They are often easier to attack using social engineering and a small hit can easily prove terminal. Big companies can take big fines, small companies can't.

THE STICK (There are no carrots)

Whilst GDPR allows for fines of up to 4% of global annual turnover up to €20m, penalties are graded and graduated. For example, failing to report a breach can result in a fine of up to 2% of annual turnover up to €10m whilst negligent handling of data can attract the top punishment. Anyone who interacts with data is liable in the event of a data breach whether or not they are themselves in the EU.

Outsourcing will not remove liability. Trying to farm out responsibility will not work. Regulators are making it clear that they will have a low tolerance of post-event finger pointing. The UK regulator has stated that company directors should be held personally responsible for data breaches and that they should be prosecuted where negligence is present.

How will you, as an individual, deal with a criminal conviction which you receive because someone in your company, who you didn't know, was doing something you didn't know they were doing. This will be a real risk for executives under the GDPR where negligence is determined to be behind a breach of data.

THE REQUIREMENT

There is a lot to do. Here are some of the things (far from exhaustive) you will need to address:

- Who in the company is responsible for GDPR compliance?
- Does the company already have comprehensive InfoSec and associated standards of protection?
- Exactly what data you hold?
- Exactly where it is held?
- Exactly what you are doing with it and do you have the necessary permissions?
- Do you have effective purge and delete policies and are they fit for purpose?
- Breach response plan?
- Breach notification procedures?
- Right to be forgotten?
- Transparency and disclosure policies?
- Transfer procedures?
- Staff & Contractor training?
- Third party validation?

Major challenges lie ahead. The GDPR stipulates that "state of the art" defences must be 'in keeping with the nature of the data and the risks to it'. That's a, 'how long is a piece of string' conundrum but is entirely predictable given the plethora of technical 'solutions'. This will provide plenty of work for lawyers but, broadly, enterprises will be left alone to decide how they should protect their data. In the event of a breach, it will be down to the breached company to demonstrate that they did everything they reasonably could to avoid a data breach. It will then be for individual regulators to rule on whether the defences were adequately 'state of the art'. The risk comes where companies try to cut corners. Regulators will be looking hard for negligence. It is easy to see how, in this situation, the victim of the data breach may well come off badly. There will be many grey areas where interpretation will be the challenge, enterprises will not be locked into any particular mandated level of technology. Simple cyber hygiene practises harvest the best improvements in InfoSec outcomes, so this approach may prove to be highly effective in the longer term.

There is much to do and little time to do it. Preparation for the GDPR is not just about available time. The GDPR is not a list to be checked off. It is also about understanding the various steps companies will need to make to achieve compliance. Many, but not all, companies will need to appoint a Data Protection Officer (DPO) and that officer will need to have a good understanding of the GDPR plus a thorough knowledge of the company's data footprint. That knowledge can only be gained from experience so if you are one of those organisations that has to appoint a DPO, they will need to be hired with enough time for them to become familiar with your company's arrangements. If you are not a company that must have a DPO, you will still need to be able to produce all of the information on demand to the regulator – and, maybe frequently, to private individuals and companies who request information on what data you hold on them. If you use Third Party contractors, particularly if that contractor is based outside of the EU, you will probably need to start policing the arrangements in place with them – remember, they may react slowly, they not be able to provide what you need (but have to have) and you may not have alternatives immediately available – 24th May 2018, is not the time to find this out!

Keep in mind that 95% of breaches are initially created by insiders, whether by accident, carelessness or dishonest design. Most of these events will be viewed by regulators as negligence – employees should have been trained and procedures should be in place to prevent these. Technical solutions are of little use if employees can't use them safely. There is too much faith in technical defences, mostly built upon false confidence regarding the efficacy of the software against modern malware or in the hands of employees who are insufficiently skilled in its use. A combination of engaged management, good governance and effective education & training is a critical aspect of your Information Security efforts and will play a major part in ensuring that your company is less likely to be targeted by cyber criminals and that, if you are attacked, you will respond efficiently and effectively. If the genesis of such a high level of data breaches is in the workforce, the focus on fixing the problem must be on ensuring unforced errors don't occur.

OUR ADVICE

Make your company compliant well before 25th May 2018, and advertise the fact that you take your data security seriously.

Talk to BeCyberSure. We can assist you in all aspects of your preparations relating to compliance with the GDPR and other InfoSec requirements.

www.becybersure.com

Twitter: @becybersure