CIO in association with Symantec

# EU GENERAL DATA PROTECTION REGULATION

After several years of negotiations, sometime towards the end of 2015[1] will see the introduction of the most important piece of privacy legislation unveiled by the EU for 20 years, the long-awaited General Data Protection Regulation (GDPR). Officially, it's an overhaul and extension of rules and principles set out in the 1995 Data Protection Directive (95/46/EC), but in scope and enforcement it breaks important new ground. Despite its unassuming-sounding title, the GDPR is set to transform data governance in the EU and beyond for a generation to come.

If the fine detail and timescales for implementation are still being argued about the outline of its most important principles is abundantly clear. Every organisation that handles the personal data of EU citizens and employees - including non-EU firms that operate inside its borders - will have to comply with a single set of rules across all member states that dictate how data must be acquired, stored, secured, and the rights of individuals to, access, challenge and have it amended.

*Fines for non-compliance, could reach up to five per cent of global turnover*

The intention is that in time organisations of all sizes will be required to comply, but initially those with more than 250 employees will face the toughest requirements. As with every EU instruction that comes with the word 'regulation' attached, compliance will be mandatory for all member states. Although yet to be agreed it has been suggested that fines for non-compliance, levied by national data protection bodies in each country, could reach up to five per cent of global turnover or €100 million (approximately £80 million), whichever is larger.

Why is the GDPR necessary and what are its aims? The simplest answer is to impose a single set of rules across the EU at a time when data has become a fundamental building block of commerce. Organisations (called 'data controllers') currently have to struggle with a patchwork of regulations in each of the EU's member states which generates huge complexity, expense and legal uncertainty. This hinders the operation of the single market, which is designed

1. As of January 2015, timescales for finalising the General Data Protection Regulation (GDPR) are unclear, as is the detail of some of its provisions. The timescales and definitions in this document are advisory only.

to make it as easy as possible for capital, people, and increasingly data, to move freely between them.

A second intention is to safeguard the privacy of individuals in an increasingly data-driven economy, a citizen-centric design that has major implications for data governance as well as planning for incidents such as data breaches. Organisations will be required to guarantee data to standards that go far beyond the informal and inconsistent processes applied today.

*For CIOs the battle is to work out how to turn the GDPR's demands into a practical plan*

For organisations that have had to deal with a mish-mash of national and EU data protection laws, the GDPR poses a major challenge to understand its requirements, assess complex new types of risk, and achieve compliance regardless of how far down that road those organisations believe they have travelled. For CIOs the battle is of a different but no less tall order - to work out how to turn the GDPR's demands into a practical plan in which their organisations buy the right security systems, set up the right data governance regimes and replicate all of this across their supply chain and partners. Given the potential for large fines, achieving this will be essential to minimise the risks of non-compliance.

## The business benefits

Despite the daunting workload, there is a wide consensus that the GDPR offers huge long-term benefits, including reduced costs for businesses operating across borders, hugely-simplified bureaucracy, and the knowledge that every single competitor - including non-EU firms that do business inside its borders - must meet the same tough requirements. The EU's own figures put the savings at €2.3 billion (£2 billion) per annum across the economic zone although against this should be set the short-term costs of implementation. The Regulation will undoubtedly be a hard road but it is one that advocates argue will be worth the journey in the end.

## Uncertainties

As of early 2015, some details remain to be agreed, as do the precise timescales for the GDPR's full implementation - with a draft due in early 2015 many experts don't see it reaching a final form until sometime between Spring 2015 and early 2016 at the latest. After that there will be a bedding-in period where prosecutions by data protection bodies such as the UK's Information Commissioner's Office (ICO) will probably be used to 'educate' and adjust organisational behaviour that falls short of the required standards.

Another issue to be thrashed out is how complaints are handled by the data protection agencies in each country. That should be straightforward where an individual is dealing with one data processing organisation in his or her country of origin, less so if that body is based in another country.

## Privacy, consent and rights

At the core of the GDPR is that organisations implement and document policies of data privacy to meet the rights of the individuals whose data they process, whether they be citizens, customers or users (called 'data subjects'), which makes it essential to work out very clearly which data qualifies as identifiably personal (including biometric and, future, genetic data), why they are collected, for what purposes are they being used, where it is stored and in what state.

*Controllers will also have to fully document all their data processing operations*

Organisations will have an incentive to collect only the data they need and take great care to ensure that it is accurate and if possible, anonymised. Failing to do that - or any of the other lifecycle provisions mentioned here - could result in major business risk. Making guesses or building on past assumptions will be a recipe for danger. All of these requirements could impose huge costs on unprepared businesses.

## Right to be forgotten

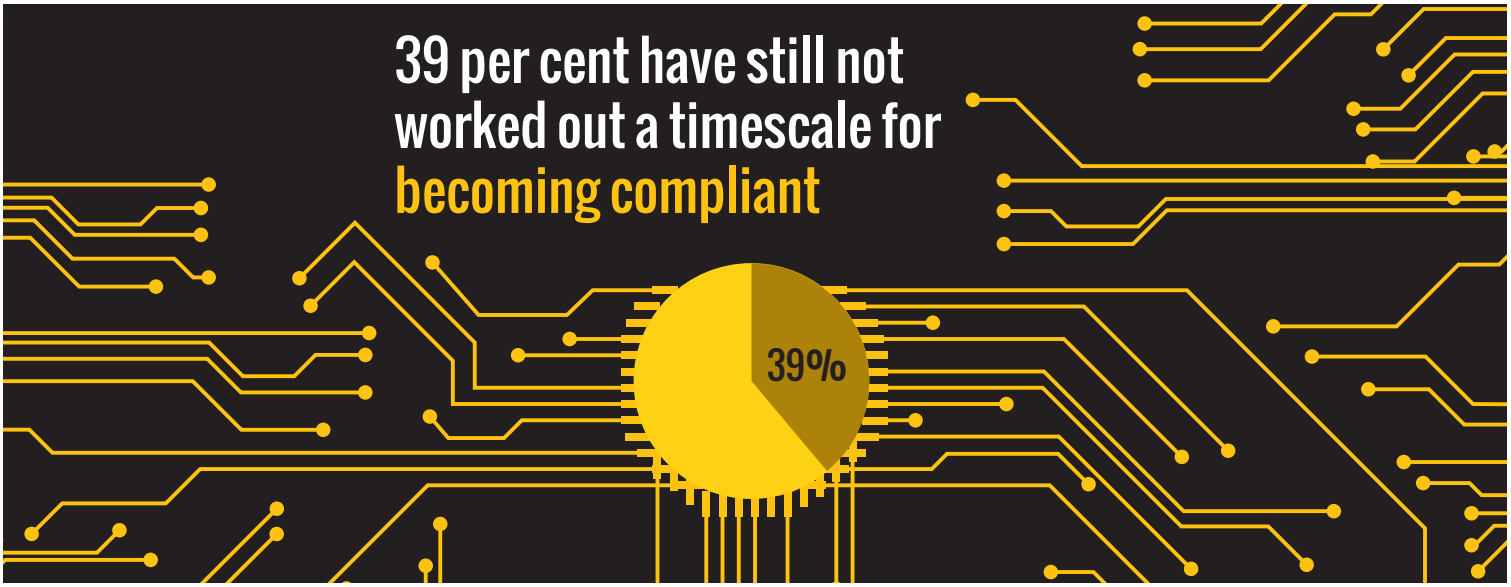
The 'right to be forgotten', backed by a European Court of Justice (ECJ) ruling in May, has attracted widespread attention as search engines such as Google have found themselves trying to accommodate the rights of individuals against other public interests such as freedom of expression and journalistic freedom. For most organisations this demand will equate to a much simpler 'right to erasure' in which data subjects will have the right to ask that data held on them is removed, particularly if it was gathered when they were children.

Individuals will probably end up with a broad right to object to what is called 'profiling' (building up a picture of an individual's interests and habits without consent) if a number of conditions are fulfilled and it is done in a way that makes them identifiable.

## Data governance

It follows that organisations will have to continue to impose the same levels of data privacy and security controls even when data is moved around or processed offshore while reviewing the mechanisms currently used to achieve this. Until recently, data moved to the US under Safe Harbour agreements would have been considered safe without question but the Edward Snowden revelations have shaken trust in this regime. Whether data is being transferring between companies, between countries, and particularly outside the EU - for example to a cloud provider - the data controller will have to tighten current due diligence on the privacy and security standards of all parts of the chain.

Controllers will also have to fully document all their data processing operations as this will replace current obligations to notify data processing to data protection authorities.




## Data protection officer (DPO)

The appointment of a data protection officer is likely to be a mandatory requirement, including in time for organisations with fewer than 250 employees if they work with more than 5,000 personal data records in a year. For larger organisations such a post will probably already exist in some form and will simply mean adding the job description to an existing post. Others might prefer to use external consultants. It will fall to this person to carry out many of the impact assessments implied by the above rules and, if necessary, help to develop the 'privacy by design' structure in conjunction with the CIO. This is a public-facing post so their contact details must be accessible.

## Data breach notification

Article 31 requires the mandatory notification of a data breach (in the UK to the Information Commissioner). The timeline has not been finalised but it is likely that notification will be required within 72 hours. There remains some doubt about how the letter of this law will be applied to large organisations, where breach investigations could be complex and time-consuming but it is clear that the days when businesses could keep incidents to themselves are coming to an end. Data controllers need to consider what internal processes will be necessary to meet the requirements of a mandatory breach notification regime.

The potential for hefty fines under this article represents a major financial and reputational risk should customers need to be informed.

## Understanding changed rules

A major issue remains the GDPR's timescales and the fine detail of its provisions, some of which are still up in the air at the time of writing. How it will be implemented over time is also hard to predict with any precision, which adds up to troubling uncertainty. This can be confusing for businesses trying to separate new provisions from ones that have existed for some time but which haven't until now come with the potential for mandatory disclosure, enforcement or fines.

"This uncertainty will be there for a while especially as the cross-border processes kick in through things like the one-stop-shop or the consistency mechanism, that is how data protection authorities make decisions on cross border issues," says Ilias Chantzos, Symantec's EMEA Director of Government Affairs programs.

"As jurisprudence and case-law develops this uncertainty will diminish but clearly from a business standpoint being a test-case is not a very good position to be at." Chantzos expects larger and multi-national organisations to "prepare for a relatively high level of compliance as a way to mitigate risk."

Symantec's Chief Strategist for EMEA Siân John echoes this, underlining that organisations, including SMEs, need to pay close attention not just to the letter of the GDPR but the changed atmosphere it will bring in its wake.

"Although data protection regulation has been around for a while the fines and consequences for non-compliance haven't been punitive. The breach notification requirements and fines are concerning businesses, particularly the efforts they will need to take to be compliant," she says.

Both Chantzos and John agree that incident management, especially of data breaches, will become a huge focus for all businesses. Although not a new concern, the likelihood of significant fines means that effectively managing such events will have a major influence on security design and buying decisions going forward. The GDPR doesn't assume that breaches suddenly become impossible, simply that organisations have taken every possible step to reduce the risk to personal data.

> *"The emphasis will be put on mechanisms that protect personal data"*
>
> *Ilias Chantzos, Symantec's EMEA Director of Government Affairs programs*

"The emphasis will be put on mechanisms that protect personal data and in the case of a breach ensure that due diligence can be demonstrated to have been in place to prevent the breach," comments Chantzos. "A focus on mobile security, encryption, identity management, compliance and cloud security are likely to be additional considerations on top of the traditional cyber-defences," he predicts.

## What next? Symantec's recommendations

1. Implementing the GDPR is a board-level issue even for larger enterprises and SMEs alike and compliance processes must be agreed at this level. Some of the GDPR's details have yet to be agreed so the board must be ready to react to any new demands when these requirements become clear.

2. Form a governance group under the direction of the Data Protection Officer and CIO. A key task will be identifying the flow of personal data into the organisation and how it is processed, stored and deleted. Current data flows, processes and policies will need to be documented, and may need to be re-engineered to accommodate new requirements, such as the need to give access to personal data in a portable form and mandatory breach notification.

3. At all stages in the lifecycle of data processing, it will be important to consider whether the level of security offered by current policies and procedures will be adequate to offer protection against unauthorised processing.

4. Assume a 'privacy by design' stance when re-engineering processes, policies and where relevant, products and services that involve the processing of personal data. If at all possible, compliance should be something that happens by default.

5. Review any breach notification process to assess whether the CTO has tools on hand to investigate the broad extent of any compromise to meet a possible 72-hour notification deadline.

## Awareness - are UK businesses prepared?

Recent research by CIO UK on behalf of Symantec found that while awareness among UK decision makers of the Regulation's imminence was high, preparedness remained a work in progress. Although the majority had started assessing the GDPR's impact, that left 31 per cent confessing that they still had considerable work to do.

Not surprisingly, 80 per cent said they were already aware of the possibility of eye-catching penalties, and 94 per cent of the potential impact of this on reputational risk. Despite this, 39 per cent had still not worked out a timescale for becoming compliant, a vagueness that is probably explained by uncertainty about the GDPR's implementation timetable.

*"Although data protection regulation has been around for a while the fines and consequences for non-compliance haven't been punitive."*

*Siân John, Symantec's EMEA Chief Strategist*

On that theme, around half of organisations believed achieving compliance would be a struggle with nearly a quarter agreeing that "they had a lot of work to do". On the Regulation's technical demands, just over half had yet to appoint a Data Protection Officer - including many among large enterprises - while a further quarter had concerns about the security training of their frontline staff.

On a positive note, 86 per cent of respondents believed that the Regulation had the potential to drive efficiency and cost savings.

## Encryption everywhere

The regulation doesn't tell security teams which security systems they should buy, only the rules under which they must be managed. It is up to organisations to interpret the GDPR's demands for themselves. Encryption is an obvious stand-out, which as numerous data breaches have demonstrated is currently often only applied to PCI DSS-mandated data such as credit cards. This will no longer be good enough; organisations will need to plan to start encrypting all personal data. This implies greater investment in technologies such as management because keys must be kept separate and secure.