CIO in association with Symantec

vanroey.be /SECURITY

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

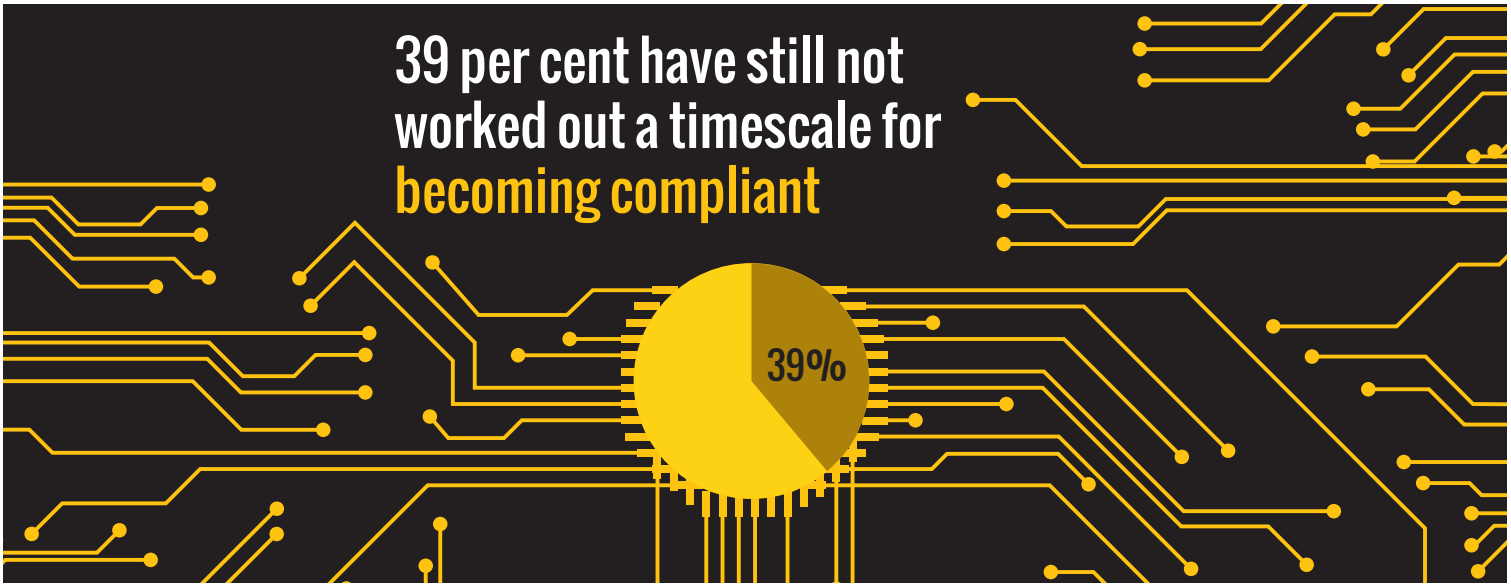
The 'right to be forgotten', backed by a European Court of Justice (ECJ) ruling in May, has attracted widespread attention as search engines such as Google have found themselves trying to accommodate the rights of individuals against other public interests such as freedom of expression and journalistic 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 & VanRoey.be'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 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.

> *"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*

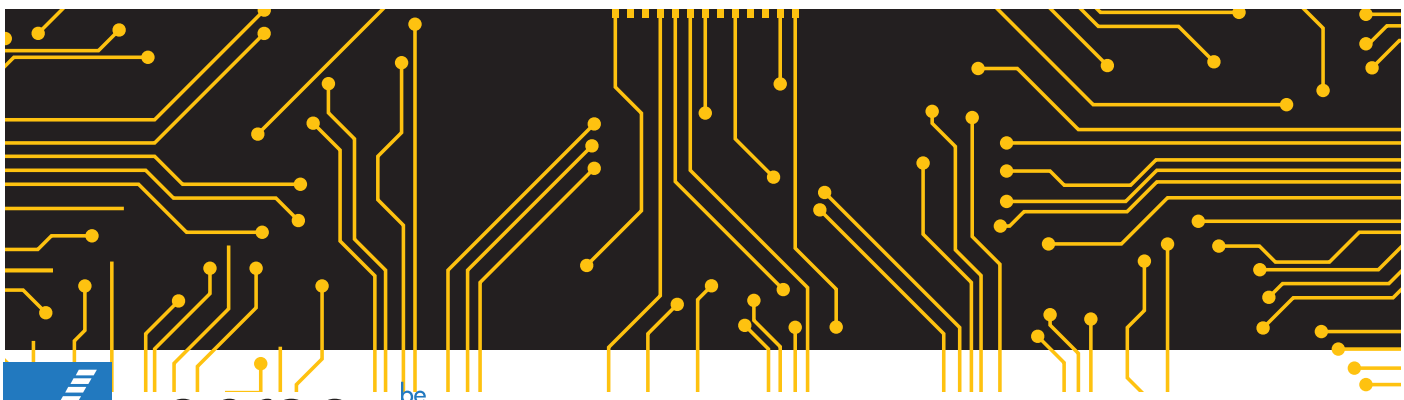
Not surprisingly, 80 per cent said they were already aware of the possibility of eye-catching penalties, and 94 per cent of the potential impact of this on reputational risk. Despite this, 39 per cent had still not worked out a timescale for becoming compliant, a vagueness that is probably explained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

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.



vanroey.be /SECURITY

The Evolution of Data Privacy

A Symantec Information Security Perspective on EU Privacy Regulations

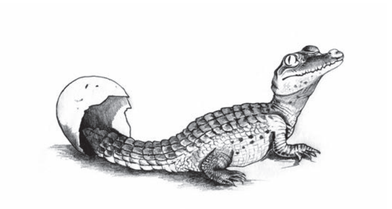
Prehistoric Protection

The European Union's proposed General Data Protection Regulation (GDPR) has left even the most informed confused. This new regulation is designed to update the current legislation which was drafted in a time that was in technology terms, prehistoric.

The Data Protection Directive, drafted back in 1995, harks back to a time when data processing was more about filing cabinets than data rack enclosures. It's time to evolve.

Today's explosion of data has meant many businesses, and even individuals, have lost track of the data they control, own, or process. As citizens, the advantages in terms of convenience and cost-savings which we all have gained from technological advances have been immense. Bringing our own devices, accessing apps, learning from the world of knowledge at our fingertips and interacting with others via the Internet has been liberating.

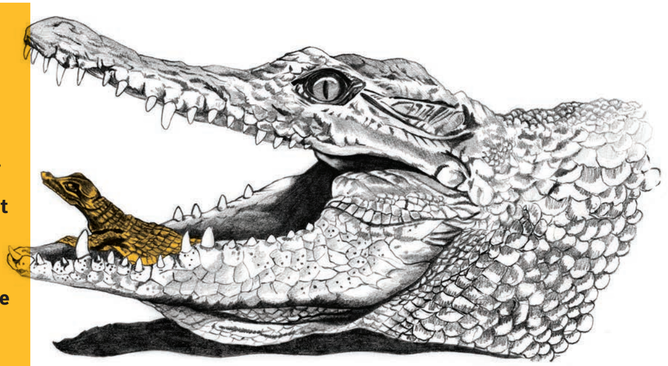
This freedom has come at a price, which is the risk to our privacy. We need to ensure we maximise the benefits from the Internet and new technology but also that we have the safeguards to ensure that this is not at the expense of our privacy.



The way our personal data is used has become a huge concern for many of us. As a major concern of its citizens, and a personal irritant to a number of its leaders, the European Union is planning to take the world of data protection in a new more considered direction.
The ramifications could be earth-shattering, costly and career-destroying. They may also be empowering and the start of a safer, more ordered, online environment.

The GDPR is still under negotiation but this perspective is based on our understanding of the current process of the legislation and the public drafts currently available. This perspective will dispel the myths, highlight the facts and inform the decisions you need to take. It is based on three undeniable facts about the EU's new proposed law:

- **It's happening.**
- **It's happening soon.**
- **And it will affect you.**



One Flew Out of The Cuckoo's Nest

Headlines about data breaches and security threats constantly remind us of the need to improve the monitoring and protection of corporate data. The volume of information gathered as we each interact with the world around will accelerate to 40 Zettabytes by 2020[1].

As it does so, public and government pressure to better protect personal data will usher in a new age of fit-for-purpose regulation.

Coming soon to a data store near you are regulations which make existing compliance measures of data privacy and protection seem very primitive. In January 2012 the European Commission revealed the first draft of its new General Data Protection Regulation (GDPR) to replace the 1995 Data Protection Directive[2]. The 1995 statute tackled the increasing complexity around data protection and storage at a time when computing was mainframe let alone wearable, when databases had rows not columns and tweeting was strictly for the birds.

The new GDPR aims to harmonise and update current data protection laws across a much-expanded EU zone of 28 counties, half a billion citizens producing $18 trillion every year[3]. If you thought things were challenging now, the impending changes for protecting personal data for all citizens will impose stricter fines on companies mismanaging data or failing to protect it properly, fines so severe that entire organizations could become extinct.

Making these changes may cause some executives to view their current data processes as inadequate or part of an era 'before recorded history'. In fact, for the first time, getting their data records in order might become a key part of their survival strategy. For others, the ability to evolve strategies, products or services which can create value from this new environment will mean their organizations thrive.

The key is to understand that anything can be personal data, particularly in the Big Data world where we can aggregate data that might identify an individual. The new rights around access and erasure, the role and liability of Data Controllers versus Data Processors are all new challenges. The good news is, we can help you with the groundwork on all of these complex topics.

The evolution is coming. Are you ready to adapt?

1. **Mandatory breach notifications**
   New draft legislation would mean any data breach involving the loss of personal data must be reported "without undue delay" within a set time frame, perhaps as quickly as 72 hours and it could be costly if you don't have the right security in place.

2. **The 'Right To Be Forgotten'**
   Sometimes referred to as the "Right Of Erasure" an idea foreshadowed by a European Court of Justice ruling earlier in 2014 forcing Google to amend some of its search results[4].

3. **Consumer Profiling Restricted**
   Citizens' data should not in principle be used without their consent. There will be no implied consent and even when consent has been given, it will be easier for citizens to retract and object to any further use of their data. This will seek to control the use of individuals' data for consumer profiling activity. As a company you need to be sure that you are using personal data safely.

4. **Be Accountable for your Data**
   Companies managing personal data may be required to hire a Data Protection Officer, implement privacy by design, understand how their data flows, and carry out mandatory impact assessments.

Up Close and Personal

What's personal has changed. Where once most work data stayed at work, and personal data at home, now both follow us around. Our personal lives are one big trail of digital clues, leaking from mobile devices as we snap, chat, pin, video, jog and log into locations every minute of our waking day. Much of this is now shared with and processed by third parties who hold this data in a new, poorly-defined, relationship of trust.

Today, the daunting reality is that in common with consumers, 50% of businesses don't realise they are losing data, let alone which data is being lost during and for up to months after a breach has occurred[5]. Soon it will be the responsibility of all organizations to protect sensitive and personal data. Fines will range from up to 5% of the organization's annual worldwide turnover to a cap of €100,000,000. Those suffering data breaches have never needed to get their information security and data storage in order more.

The new EU regulations will affect the storage and safety of 'personal data'. For the purposes of the legislation this refers to any information relating to an identified, or an identifiable natural person[6]. This means if a person can be identified directly, or indirectly, by reference to an ID number, or his or her physical, physiological, mental, economic, cultural or social data then extra protection will have to be put in place including the likely appointment of a DPO (see Box)[7].

In order to further protect and manage the protection of personal data the GDPR will require the employment of a Data Protection Officer (DPO) for businesses with data on more than 5,000 people in any 12-month period, or may even include a smaller business processing sensitive data, such as health data.

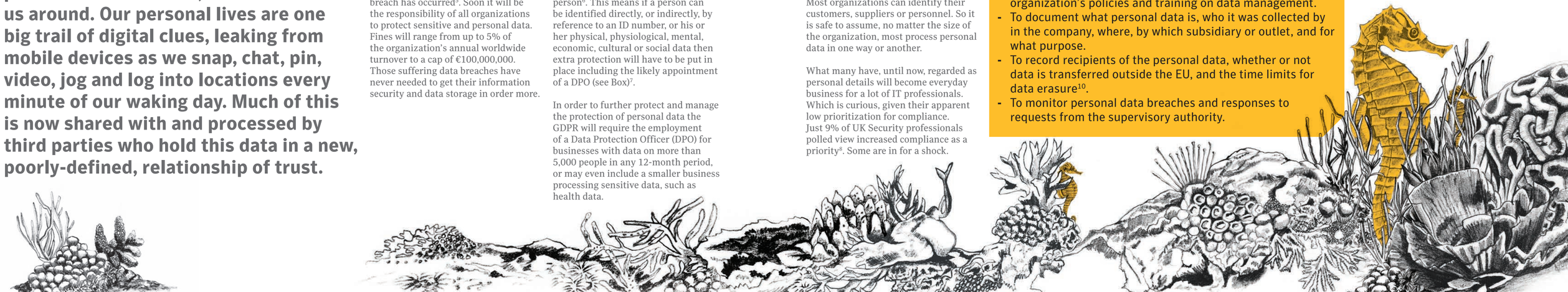
The comprehensive definition on what constitutes personal data increases the scope of the legislation to include the profiling of consumers made possible by analysing internet access or device data. Most organizations can identify their customers, suppliers or personnel. So it is safe to assume, no matter the size of the organization, most process personal data in one way or another.

What many have, until now, regarded as personal details will become everyday business for a lot of IT professionals. Which is curious, given their apparent low prioritization for compliance. Just 9% of UK Security professionals polled view increased compliance as a priority[8]. Some are in for a shock.

What's a DPO?

For organizations collecting the personal data of EU citizens, Data Protection Officers are designated persons responsible for making sure the organization follows the new regulations. Pending the finalization of the reforms in 2016 DPOs will have several duties:

- To inform and advise the company of its obligations and to document this activity and the responses received.
- To monitor the implementation and application of the organization's policies and training on data management.
- To document what personal data is, who it was collected by in the company, where, by which subsidiary or outlet, and for what purpose.
- To record recipients of the personal data, whether or not data is transferred outside the EU, and the time limits for data erasure[10].
- To monitor personal data breaches and responses to requests from the supervisory authority.



The Next Generation of Privacy

The proposed Data Protection Regulation enshrines the "Right To Erasure" but that's not all. It is a fundamental modernisation of Europe's data protection rules taking into account the huge data evolution of the last 20 years. Having an understanding of the personal data you have, where and why it is stored makes sense. Not only will this understanding protect the individuals to whom the data relates, but also the organizations responsible for its protection. Two key concepts are the "Right Of Access" and the "Right To Be Forgotten".

The proposed regulation, for the first time, leaves no legal doubt that the physical location of a server, or a company processing data is irrelevant to the application of European data protection law. The new GDPR applies globally, not just to Data Controllers located in EU member states.

European residents buying a service or product, where personal data is stored, will be protected, regardless of where they, or their data, are in the world. What becomes simpler under the new regulation is that companies can now comply with one pan-European law rather than with different interpretations in different member states.

This makes it easier for those operating in all countries, but may affect those who have only operated in states with more liberal interpretations of the current directive.

When services are being offered to consumers in Europe, European regulations will apply. Rather like the pre-Jurassic super-continent Pangaea, European consumer data is regulated by European regulation no matter where you, or your data, may travel in the world.

From its inception, the GDPR provides individuals with the right to have their data erased under the following circumstances:

- The data is no longer necessary in relation to the purposes for which it was collected or processed.
- An individual withdraws consent for the processing.
- When the storage period consented to has expired.
- The data subject objects to the processing of personal data.

Right Of Access -
Individuals shall be guaranteed the right to obtain from the company the rectification, erasure or blocking of personal data concerning them.

Right To Be Forgotten -
It is now for the organization and not the individual, to prove data cannot be deleted because it is still needed or relevant.

Controller versus Processor

The new regulation, like the one it replaces[9], impacts both 'Data Controllers' and 'Data Processors'. The definition recognises not all organizations involved in the processing of personal data have the same degree of responsibility.

Data Controllers must exercise control over the processing and carry data protection responsibility for it. Data Processors also have detailed obligations.

So, which are you?

To make this a little more complex, some organizations may be considered both Controller and Processor. In fact it is more than likely you are both.

The distinction between a Data Controller and Data Processor has significant real-world consequences. For example, following a data breach it is essential for both to determine where responsibility lies.

Therefore, it is important that organizations involved in data processing activities establish their roles and responsibilities at an early stage, preferably before processing commences.

Which are you?

Data Controller -
an organization who (either alone or jointly or in common with other organizations) determines the purposes for which, and the manner in which, any personal data is collected, or is to be processed.

Data Processor –
any organization (other than the data controller itself and its employees) who processes the personal data on behalf of the data controller.

Processing -
any activity consisting of obtaining, recording or holding personal data or carrying out any operation or set of operations on such data.

To determine whether you are the data controller you need to ask:

- Why do we collect personal data and what is our legal basis for doing so?
- What will the data we hold be used for?
- Which individuals do we collect data about?
- To whom do we disclose the data, and under what circumstances?
- Which subject access and other individuals' rights apply taking into account exemptions?
- How long do we retain the data, and do we make non-routine amendments to the data?

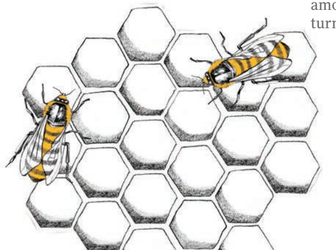
Clean Little and Often

Finding out where all this Personal Data is, how it flows around your organization and who has access to it is something many organizations struggle with. Four simple questions demonstrate the scale of the issues that GDPR compliance may present to organizations:

- **What data do I have?**
- **Where is the data stored and for how long?**
- **Who has access to it?**
- **Am I using it for the reason I originally collected it?**

Today very few organizations could provide a satisfactory answer to those, let alone to the depth needed to become compliant with the new General Data Protection Regulation. With the consumerization of IT rife within the majority of organizations today, many would struggle to understand not just where, but how, their data flows and proliferates around their organization.

But all is not lost. If we look at data management as being akin to doing your tax declaration or a spring clean you can begin to understand the benefit of automating data retention, storage and back-up.

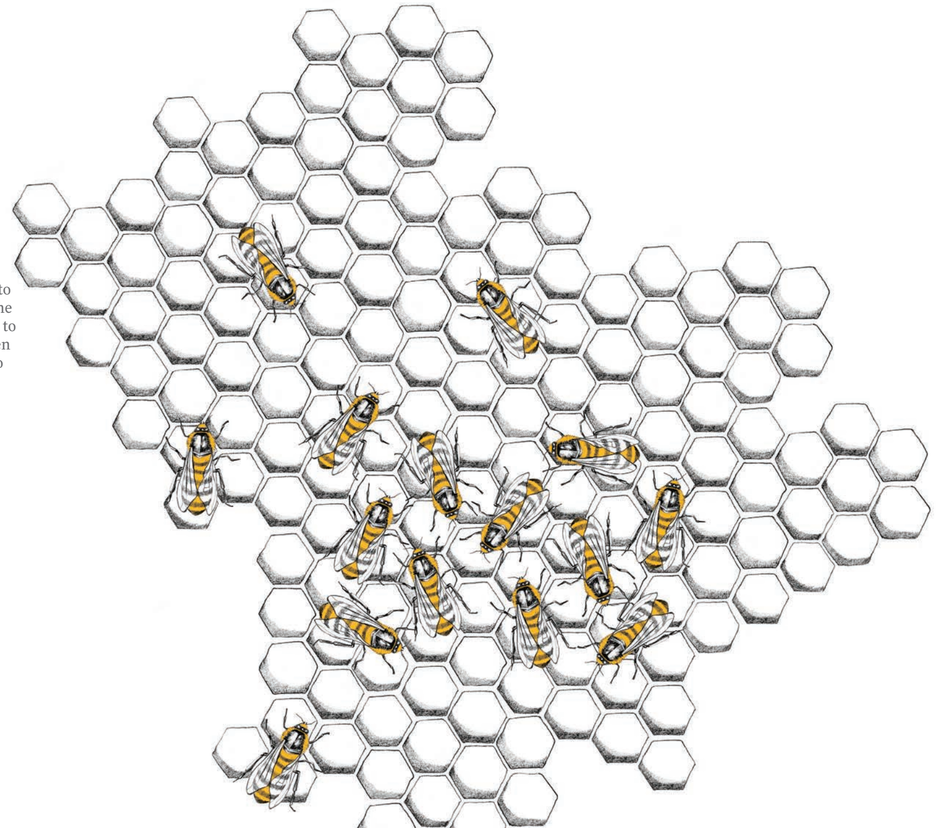


Many of us will have experienced the difficulty of completing our annual tax declaration on time and accurately. The simple process of finding, collating and understanding what we have earned and spent over the last year in order to document it for the authorities[11], leaves many up to their eyeballs in unrecognisable receipts or calling in an expensive third party to manage the process.

In the context of your annual 'spring clean', waiting all year to sort through your house, cleaning the attic or sorting out the garage can become daunting. What would be a quick job if a small amount were done every day, instead turns into a cleaning ordeal.

By reviewing, storing and collating data daily, you will be in the position to prove quickly that you are on top of the data management procedures needed to meet the GDPR . This is essential when you are audited, or should you have to prove compliance to the authorities.

You may not be surprised to hear that many companies are storing far more data than they actually need, including duplicates or out-of-date data which add unnecessarily to the burden of compliance. Not only will understanding the new legislation reduce the risk of heavy fines or legal action, but knowing what should be kept and what should be disposed of will vastly reduce your storage needs and associated costs.



Ban Tick Box Mentality

Don't wait for the legislation. Look at what you need to protect today and this will prepare you for complying with the regulation. The GDPR is looking to ensure that the privacy of personal data is protected.

Ensuring you implement the best practices and have built in privacy by design will make you more prepared to comply with the regulation, will reduce your risk and costs making you more agile.

A common mistake, but a traditional way of dealing with conforming to stipulations and regulations, is a checklist. A tick box mentality to compliance with brand new regulations as broad as the GDPR is unlikely to succeed. So when designing your privacy protection here are eight key considerations:

1. Where, how and why are you storing personal data?
2. Which IT systems or other methods are used to collect personal data?
3. Which security processes protect the personal data you store?
4. How do you transfer the personal data from one organization to another?
5. How do you retrieve personal data about certain individuals?
6. How do you ensure a retention schedule is adhered to?
7. How do you delete or dispose of the data?
8. Can you control the personal data you use across your business from creation to deletion?

Unfortunately it's never that easy! Even with the appropriate answers to the above questions you will not be protected. Whether you are required to appoint a Data Protection Officer or appoint one to help with the transition and management of the new regulations it will be more than ticking boxes. The reality is this reform has been a long time coming. The original mandate focused on the paper data we stored in old-fashioned filing cabinets, the world we see today has evolved significantly.

Until now, there have been few industry drivers to take data privacy and security seriously, unlike other regulatory issues such as PCI compliance or Sarbanes Oxley, which is why the EU stepped up. Rather than challenging yourself with 'How do I comply with the regulation?', look at how your data should best be secured. Doing so will likely achieve early compliance.

Organizations are starting to take the issue of personal privacy seriously, but there is no 'one size fits all' solution.

Focusing on the business outcome you are trying to achieve and gain an understanding of the risk specific to your organization is critical.

When the checklist becomes 'Business As Usual' and compliance becomes an organization-wide quality standard, it can build into competitive advantage.

- Do you manage high volumes of personal data?
- Are you in an industry with highly-sensitive information?
- Will hackers expect lower security standards in your sector?
- What data do you need and what are you storing unintentionally?

You Can't Outsource Risk

Today security breaches and privacy issues are more regular, more serious and more damaging than ever. So when the worst hits where does the buck stop?

As several banks and retailers have found to their cost, it is your brand on the front pages of the papers when a breach is unveiled, seldom those providing your IT and services.

Of course, no sane manager would knowingly take great risks with IT Security, so it is wise to ask where the unknown risks, which some call Black Swans[12], lurk. Many malicious attacks, the sort which would contravene the EU regulation, would traditionally be internal, from disgruntled employees for instance. In other cases the threats are often outside your organization and driven by factors outside of your direct control.

Take the case of cloud providers. When negotiating your contracts it helps to understand the very small amount of wiggle room many low-cost cloud services have in such a competitive market place. It may foster an attitude such as "You're only paying me £5,000 a month why should I offer unlimited indemnity, given the risk of EU non-compliance?'

They have a point, because you are still the Data Controller and ultimately responsible for the security, handling and privacy of personal data. Passing the parcel, when it's a data packet, does not work.

Under the GDPR, the same will apply to Software as a Service (SaaS) providers. They are expected to take privacy seriously as their business is built on processing customer data. Often they provide very strong security credentials. However, no matter which Service Level Agreements they provide, the Data Controller, will still be responsible.

For example, consider the very customisable privacy settings available to Facebook users today. Then consider how many users fully enable it.

Important questions to ask yourself when outsourcing IT:

1. How could I get my information out if I needed to?
2. How can I guarantee personal data is deleted?
3. What issues could emerge from a data breach by my supplier?
4. What is the process for informing my suppliers should I have a data breach?
5. Do I know how data flows in and out of my cloud and/or SaaS providers and do I have the right contracts?

Conclusion

Today most organizations handle personal, and other sensitive information. The GDPR will force businesses to take precautions in processing personal data to a new level. It will pay to remember for which data you are Data Controller and Data Processor, bearing in mind you may be both.

This isn't at all straightforward for enterprises, thanks to their poor information processes. For instance, if a third party is subject to a breach then you may be able to sue your suppliers, but ultimately it is your organization that will be accountable to the Data Protection Authority. This means organizations must now take the legislation seriously and most importantly plan now to comply with it.

We need to embrace the law not just pay lip service to it. With a rise of consumer grade cloud storage, social media and a world of targeted advertising, data is given away, shared and generally used as a commodity the world over.

Without understanding the data your organization owns and shares, it will be impossible to meet the new regulation.

For each organization the solution to securing information will differ, but there are common themes to a successful approach to the GDPR:

- Embed GDPR compliance into your security program. This will simplify and drive efficiency of the GDPR project.
- Secure enterprise data holistically, not one step at a time, project-by-project, or function-by-function. This should be driven by the business as a whole, not just IT, to evolve security behaviours across the organization.
- Undertake appropriate due diligence for new suppliers, systems and processes and make this a cornerstone of information governance.

Fortunately, compliance with the GDPR will assist not only with protecting the personal data of individuals, but also businesses with defending against the increasingly targeted Cyber attacks. Symantec recommends a risk-based approach to complying with the GDPR. A side-effect may be to liberate information security professionals from the mundanity of defending the indefensible by emphasising a new focus on protecting personal data strategically.

For those who survive the evolution, there are clear competitive and reputational benefits that come from being seen as a responsible organization that can be trusted with a consumer's personal data.

The Evolution of Data Privacy

The EU's new General Data Protection Regulation has left many businesses wondering if they are ready to comply.
Here are the reasons why.

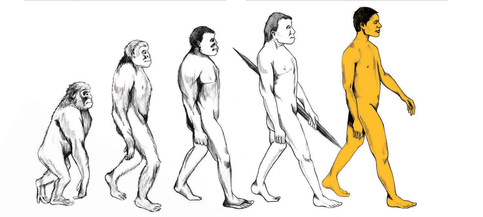
Data Growth is at an all time high and only getting bigger

2010

1.2 Zettabytes
in the Digital universe

2020

40 Zettabytes
in the Digital universe



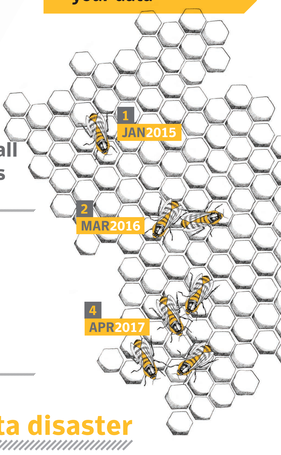
Are you ready to adapt?

- ☐ **Mandatory Breach Notification**
- ☐ **The Right to be Forgotten**
- ☐ **Consumer Profiling Restricted**
- ☐ **Be accountable for your data**

The DPO

The volume of business data worldwide, across all companies, doubles every 1.2 years.

Data Protection Officer will be required for businesses with data on more than 5,000 people.



A dawning data disaster

50%
of businesses don't realise they are losing data

of these:

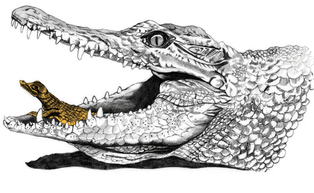
50%
of targeted attacks by phishing are on large enterprise **(2,501+ employees)**

16%
Public administration **(Government)**

15%
Professional services

The complacency challenge:

9%
of UK security professionals polled seeing increased compliance as a priority



Your personal data challenge

- **What data do I have?**
- **Where is the data stored and for how long?**
- **Who has access to it?**
- **Am I using it for the reason I originally collected it?**

Source: Symantec Annual Threat Report and Wikibon Blog (Big Data statistics)

Symantec EMEA Headquarters,
350 Brook Drive,
Green Park,
Reading RG2 6UH
Tel: +44 (0)870 243 1080

References

1, and **8** - Symantec Vision London 2014 “The low down - what we learnt from you” - www.symspace.co.uk/blog?id=7694
2 EU Data Protection act - Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)
3 Wikipedia - www.wikipedia.org/wiki/European_Union
4 BBC News Europe, 13th May 2014 - www.bbc.co.uk/news/world-europe-27388289
5 2014 Verizon Data Breach Investigations Report p.21
6 EU Data Protection act, Page 41, Article 4 - http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf
7 European Parliament legislative resolution of 12 March 2014, recitals 75 and 75a - http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0212&language=EN&ring=A7-2013-0402
8 EU Data Protection act, Page 65, Section 4, Article 35 - http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf
9 UK Information Commissioners Office ‘Data Controllers and data processors: what the difference is and what the governance implications are.’ - www.ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf
10 EU Data Protection act EU Data Protection act, Page 66, Section 4, Article 37 - http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf
11 UK Financial Conduct Authority website - www.fca.org.uk/news/fca-fines-five-banks-for-fx-failings
12 The Black Swan: The Impact of the Highly Improbable, Nassim Nicholas Taleb, 2008

Symantec

vanroey.be /SECURITY

www.VanRoey.be/Security // Business@vanroey.be // 014 470 605
Blarenberglaan 6 - 2800 **Mechelen**
Kempenlaan 2 - 2300 **Turnhout**
Antwerpseweg 116h - 2440 **Geel**