clearswift

Preparing for GDPR

Frequently Asked Questions & Answers

July 2016

Contents

Background

The new European Union General Data Protection Regulation (EU 2016/679) is coming into force in 2018, requiring a level of data privacy and security that is beyond what most organisations are currently equipped to manage. If you do business in the EU, even if you don't have a presence, then you must sort through the prescribed compliance measures or risk facing hefty fines.

Clearswift offers a number of GDPR resources that will help you clarify the regulation and streamline your preparation. In addition to our detailed Clearswift whitepaper 'Preparing for the EU Data Protection Regulation. Regulation Overview and Technology Strategy, and on-demand webinar co-hosted with Forrester, we have summarized a few of the most frequently asked questions surrounding the GDPR below.

Questions & Answers

1. Why is the GDPR being put in place now?

The EU has had a directive on data protection[1] and privacy for more than 20 years. It is a cornerstone to both EU privacy and human rights law and covers many of the same topics that GDPR covers. However, the implementation of the law is up to the member states, as a directive it is not legally binding. The value of information, the way it is shared and managed has changed a great deal over the past 20 years and there is now a need for a regulation rather than a directive. One which is legally binding and also creates consistency across the whole of the EU.

Far from being a burden on doing business, GDPR is expected to save more than €2 billion per year as there will just be a single set of rules to comply with rather than different ones in different countries.

2. When does GDPR come into force?

The regulation will come into force in Spring 2018. While this may seem to be a long way off, in terms of larger compliance projects it is just around the corner. If there needs to be capital expenditure, then there is probably only one more round of planning which can result in time required for research, purchasing and implementation

3. What information needs to be protected?

GDPR is about protecting EU citizen personal data. However, the definition of personal data is often the subject of debate. The European Commission defines personal data as[2] *"any information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer's IP address."*

It's important to note that special conditions have been outlined for the processing of data related to national security, children protection, healthcare, historical and scientific research purposes.

4. Won't the proposed fines put organizations out of business?

The fines should a compliance breach occur have been headline grabbing – and at 4% of global turnover this could absolutely result in a company going out of business. However, the fine is designed to focus the mind towards achieving compliance, rather than having to pay it. There are other precedents for paying very large fines, for example the recent Volkswagen emissions settlement in the United States.

Cyber security needs focus, and at a boardroom level – the fines will certainly provide the impetus to acting on it rather than just talking about it.

[1] https://en.wikipedia.org/wiki/Data_Protection_Directive

[2] http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en

5. **Will the fines really be enforced?**

As none have been imposed yet, there is a certain amount of speculation. However, currently different countries have imposed fines for data breaches and often these have been to the maximum amount that has been allowed. The general consensus is that there will be a very large fine imposed early on as a means to 'encourage' organizations' to comply.

Of course, the goal of compliance is to avoid the fine. Spending time considering the possibility of a fine will only decrease the amount of time you have to become compliant.

6. **Is a firm required to store and make accessible an individual's specific consent provision – i.e., the form itself?**

There are multiple ways in which the individual can comply to the request, it might be through a paper form or it might be from an online web page. The onus is on the company to be able to prove consent and so it is up to them as to how best achieve compliance. For many, it is expected that they will record the date and time of the consent being given, rather than a paper form. For those with paper forms, they will probably be scanned and archived so that they can be searched for at a later date if requested.

It should also be noted that there is also the need when dealing with children under 16 that consent needs to be given by the parents or custodians – and that this needs to be verifiable.

7. **Are there requirements for email archiving?**

No – not specifically within the regulation. However, there is a need in other regulations to keep email for a specific amount of time, especially if it is a corporate record.

If data sharing with partners is carried out using email, then an archive could be used to help track who has received what (and conversely what you have received from partners). This information is needed in order to be able to comply with specific requests within the regulation, for example withdrawing consent, aka the right to be forgotten.

8. **What does 'privacy by design' really mean?**

Privacy by design is one of the key components of GDPR. We know that, in general, security and privacy tend to be thought about after a product or application has been created and subsequently retrofitted. By designing it in from the start means that the compromises which are often made in retrofitting do not have to be made.

Jan Philipp Albrecht[3], talks not just about privacy by design but also for implementation. Currently there are no standards as to how to easily measure this and therefore it can be complex for the board to understand where they stand from a compliance perspective.

9. **By complying with the GDPR, would firms also help to mitigate their other business cybersecurity risks?**

Yes, absolutely. GDPR is not dissimilar to the 100+ other regulations around the globe relating to data protection and privacy. Its reach is further than most of those, and the impact is greater – however the essence is the same. Understand your information, where it is stored, who has access and protect it. Understand it well enough that you can control it, so if you are asked to delete it, you are able to.

Complying with GDPR will be, in effect, a superset of other regulations you may have to comply with.

10. **Does GDPR contradict other regulations?**

For many businesses, compliance with regulations is a balancing act where the regulations appear contradictory and GDPR is no exception. Understanding the regulations you and your organization needs to comply with can help uncover and clarify the position on the contradiction.

A simple example is the GDPR 'right to be forgotten'. On the face of it, this is about a request to delete all information relating to the individual who has made the request. However, if that person has bought goods or a service then other regulations will probably overrule GDPR – as there are requirements to keep those types of records for a period of time.

[3] http://www.europarl.europa.eu/meps/en/96736/JAN+PHILIPP_ALBRECHT_home.html

11. How does the GDPR deal with encryption?

Encryption is not specifically mentioned in GDPR, but it is a valuable technology for security and privacy. Information such as Credit Card numbers are required to be encrypted at various points in their handling through the PCI DSS (Payment Card Industry Data Security Standard) and this shows how it can be used in a compliance program.

There is a potential regulatory compliance conundrum when using encryption, or rather decryption, of respecting the privacy of individuals while, at the same time, conducting mandated surveillance and monitoring for potential insider dealing, market manipulation, bribery, corruption, money laundering, etc.

Encryption solutions today are designed to help businesses handle both the privacy aspects of working as well as the compliance requirements. GDPR is not designed to put this balance at risk. For many organizations having well defined polices which lay out acceptable usage is key to then putting a suitable solution in place. Within the financial services market, there are strict guidelines on what is and what is not deemed acceptable, these are then put in policies which are then enforced by individuals, departments and technology.

12. How does Britain's exit from the EU impact my data in the UK?

At this point in time (July 2016), not at all, the exit is planned to take at least two years and until the UK actually leaves, it is still 'in'. Today, there are several different rules around data in the UK about how it is stored and accessed. Safe Harbor[4] has been replaced by the EU-US Privacy Shield[5] requirements, but even if this is not applicable, then other regulations which have been around for several years can be used, such as Model Contract Clauses[6] or Binding Corporate Rules[7] (BCRs).

Even after the exit, UK businesses which deal with EU citizen data will still need to be compliant with the GDPR.

13. What's the balance between the privacy regulations of the third-parties we are to audit for privacy protections?

GDPR needs to be thought of as an enabler, which is difficult as most people see it as 'yet more regulation'. Its reach goes further than before and organizations will need to start asking questions of their partners, suppliers, contractors and consultants to ensure that the privacy rights of the customer, client or citizen are suitably protected. Asking the types of questions that will need to be asked will inevitably result in push-back. For example, providing high-level results of penetration and vulnerability tests as a means to decide whether a partner is taking cyber-security seriously could be seen as undermining their business.

We live in interesting times. One way to tackle compliance is to wonder how people are dealing with your own personal information. We always hope that they won't sell it, accidentally 'leak' it or give it away to other companies – but we don't know. We'd like to think that other organizations protect their critical information as well as we would – and this might well be the case – but you won't know unless you ask. No organization is an island, all have others upstream and downstream – so while you might not want to ask someone else about their cyber preparedness, be ready to be asked yourselves. Working together to put appropriate protections in place across the information chain will provide benefits for all.

14. Will compliance with GDPR put me at a disadvantage to those who don't comply?

If you trade in the EU then you need to comply with GDPR. The current system potentially penalizes those who have a presence in the EU over those who don't. Under the new regulation, it will be the same for both. Likewise, there are currently differences from one country to another as they interpret the existing EU guidelines differently – the new regulation standardizes it across the region which will create advantage, not disadvantage.

[4] https://en.wikipedia.org/wiki/Safe_harbor_(law)

[5] https://en.wikipedia.org/wiki/EU-US_Privacy_Shield

[6] http://www.out-law.com/en/topics/tmt--sourcing/data-protection-and-privacy/model-clauses-for-transferring-personal-data-overseas-an-overview/

[7] https://en.wikipedia.org/wiki/Binding_corporate_rules

15. Do I really need to hire a Data Protection Officer?

The short answer is 'yes.' The long answer is more involved as you could share Data Protection Officers (DPOs) with another organization or you could assign the role to an existing individual. The role of the DPO is to look at the organization from the side of the regulator, who is really concerned with protecting the information of the citizen. If you think about the DPO as someone to help drive compliance and competitive advantage through compliance, then the role is a very positive one to have.

16. We have a CISO (or a CIO), can they be our Data Protection Officer (DPO)?

Once again the short answer is 'yes.' For many smaller organizations various officers of the company will need to hold multiple roles. There is a natural fit between the CISO or CIO and the DPO. Smaller organizations are also looking at the IT Director or IT Security Manager to take on the mantle of DPO. In all cases it is worth sending the person who ends up with the role on a course to understand the details of the regulation, as there are sections which obviously fall into the skill set of an IT professional, and there are others which may require additional training to ensure the nuances are covered. For larger organizations, keeping the roles separate can help drive compliance as there is no conflict of interests.

Where do I begin?

Before getting carried away with the regulation there is a need for education and awareness. Start a cross-business working group to discuss GDPR and its requirements. When this is in place then you can put together a plan of action. Please visit Clearswift's GDPR Resource Center for additional resources on how to start your preparation.

17. Where do I really begin?

On the face of it, GDPR compliance looks like an enormous task, however starting with the basics and breaking it down into actionable chunks will make it easier. If you already comply with a variety of legislation then that will be an excellent place to begin – where are the similarities and where are the differences? In the United States there are multiple breach notification laws, and there is a requirement for breach notification in GDPR – so probably not that different for US businesses to what is done today.

GDPR is all about information and protecting it, no matter where it is. Understanding your information is the essential first step:

- What is the information you have today which will be subject to regulation?
- Where is this information stored (think beyond the database, to reports, files, cloud storage, USBs, etc.)?
- Who has access to it (not just internal, think about external people 'onsite' as well as those you send it to, externally)?
- What is the purpose for processing and what level of consent might you already have to do so?
- How can it possibly accidentally or maliciously leave the organization email, FTP, cloud storage/ collaboration, social media, published on the corporate website, etc.)?

Understanding the information and the information flows will enable a plan for compliance to be developed. Look at existing policies, processes and security solutions – which can be used as part of the compliance program, that need to be enhanced or augmented.

18. Which is the most difficult piece of the regulation to comply with?

This is a hard question to answer, however, the "right to be forgotten" is probably the toughest one. This is also known as "withdrawing consent" or "right to erasure" and is where the individual can request the removal (erasure) of all personal data relating to themselves.

From the organization's perspective, they need to be able to find the information – no matter where it is and then erase it. Providing that doesn't violate/contradict other regulations which may apply. While finding records in a database can be relatively simple, there is also a need to find other copies, which might be in email, reports and documents. The reach of GDPR also means that this request has to be 'passed onto other 3rd parties' with whom the information may also have been shared with.

While all this is completely possible with technology today, most companies don't have the processes or technology in place to comply with the request.

19. Is GDPR only a problem if you get caught?

If you deal with the EU and hold information which is regulated, then there is a requirement to document compliance and the strategies used to achieve it. The regulator can request this information at any time. Not having it will also be a breach of the regulations.

GDPR extends beyond the organization to suppliers and all those involved in the information supply chain. Requests from other organizations will become commonplace and a pre-requisite to doing business. After all, would you want to share information which was subject to GDPR with a business that was unable to prove they could look after it?

20. Will GDPR compliance cost a lot of money?

This is a difficult question to answer. If your organization is heavily regulated today, then the impact may be minimal. There may be a need to put some new processes put in place to deal with specific requests, and there may be a need for new technology solutions to help enforce new policies and new processes, but there might not.

For most organizations, regulatory compliance is going to cost both time and money. The cost of complying will be cheaper than dealing with the fine and the scramble to deal with non-compliance. Even without the new fines, Sony was estimated to have spent $171M to clean-up after their breach in 2011[8]. However, this can be used to drive competitive advantage, especially in the early days. 33% of consumers have cancelled a transaction because of a privacy concern[9]. Having better privacy policies in place than your competitors will drive people to use you rather than them.

[8] http://www.darkreading.com/attacks-and-breaches/sony-data-breach-cleanup-to-cost-$171-million/d/d-id/1097898

[9] Forrester North American Consumer Technology Survey, 2014

clearswift

Clearswift products, solutions and professional services can help you with various aspects of GDPR compliance.

Clearswift is trusted by organizations globally to protect their critical information, giving them the freedom to securely collaborate and drive business growth. Our unique technology supports a straightforward and 'adaptive' data loss prevention solution, avoiding the risk of business interruption and enabling organizations' to have 100% visibility of their critical information 100% of the time.

For more information, please visit **clearswift.com**

United Kingdom
Clearswift Ltd
1310 Waterside
Arlington Business Park
Theale, Reading
RG7 4SA
UK

Germany
Clearswift GmbH
Im Mediapark 8
D-50670 Cologne
GERMANY

United States
Clearswift Corporation
309 Fellowship Road
Suite 200
Mount Laurel, NJ 08054
UNITED STATES

Japan
Clearswift K.K
Shinjuku Park Tower N30th Floor
3-7-1 Nishi-Shinjuku
Tokyo 163-1030
JAPAN

Australia
Clearswift (Asia/Pacific) Pty Ltd
Level 17 Regus
Coca Cola Place
40 Mount Street
North Sydney NSW 2060
AUSTRALIA