clearswift

Preparing for the EU General Data Protection Regulation (GDPR)

Regulation Overview and Technology Strategy

June, 2016

Contents

Introduction

For many the initials GDPR sends a shiver down their spines. The next generation of EU Data Protection regulations, the General Data Protection Regulation (GDPR) has moved forward with agreement from member states and an enforcement date of Spring 2018. The idea of having a unified set of consistent regulations, rather than different in every member state should make things easier for most organizations. Unfortunately this isn't the way it is seen due to some of the provisions set out in the regulation.

While regulations are not usually headline grabbing, GDPR has caught the eye of the media for the substantial "teeth" it brings with it in the form of stringent and prescriptive privacy obligations, requirements to ensure policy enforcement through technical measures and the potential for hefty fines. Of course, organizations want to be in compliance with the laws of the land and avoid any possible fines, but more importantly, the true goal is to ensure they can effectively protect their critical information without excessive costs and disruption to their business operations.

This white paper prepares you for GDPR by providing a basic understanding of what is involved with the different sections of the regulations, and how technology can be used to drive the initial discovery which can be used to drive the plan as well as the ongoing process of maintaining compliance.

Background

It is over three years since Viviane Reding (Vice-president and commissioner responsible for justice, fundamental rights and citizenship) unveiled her ambitious plans to overhaul the data protection regime in Europe in the form of the draft General Data Protection Regulation.

The new regulation is a key element for the Digital Single Market, but if citizens do not trust online services, they will not benefit from all the opportunities presented by technology. Confidence is paramount, but it is still far from a reality.

The bar for compliance will be much higher under the new regime and the sanctions for not complying far greater, with fines of up to 4% of global annual turnover or 20 million Euros (whichever is the higher) proposed.

The direction of travel of the regulation, the current focus of the media and regulators on data compliance, and the scale of the compliance challenge ahead, means that organizations need to start transforming data compliance today to be ready for the new regime, avoid costly fines and damage to hard earned trust and reputations.

But what should organizations focus on and what does compliance look like? Below is an overview of the top issues under the regulation, how the proposals differ from current data protection laws and what the practical compliance challenges are for organizations.

The Regulation and You

At first sight, regulations can appear a minefield and there is no doubt that having an expert come in and help talk through them is a great idea. However, that is not always practical. So, here are the major points from GDPR which you need to consider.

Fines and enforcement

With fines of up to 4% of global annual turnover or 20 million Euros agreed (whichever is the higher), the new regime will put data protection on a par with anti-trust and anti-bribery sanctions. "Taking a view" on compliance is about to become prohibitively expensive. There is a great deal for organizations to do between now and spring 2018 (when the regulation becomes enforceable by law).

Territorial reach

The new regime will greatly extend the reach of the EU legislation. There is no way to avoid its reach. National boundaries from Sydney to Silicon Valley to Sharjah and beyond are all visible to the regulation when they handle EU citizen personal data.

There are regulations and standards which cross geographic boundaries, for example the Payment Card Industry Data Security Standards (PCI DSS), however they are very specific and for most handled in a simplified manner, for example, by using a third party payment system. GDPR is far more wide reaching, so if you are based in the United States and selling widgets to individuals in Europe, then you will be subject to GDPR. Likewise, if you have a very small business based in Scotland and are selling to hill farmers in Wales, you will be subject to GDPR.

Scope of personal data

The definition of personal data (any information related to a data subject) is set to broaden under the regulation, bringing much more data into the regulated perimeter. Changes are proposed to keep pace with the online environment (web 2.0, Internet, social apps, etc.) and rapid technological change (mobile, connectivity, etc.) which are an essential element to achieve the EU's 'Digital Single Market'. Additionally, special conditions and provisions have been outlined for the processing of data related to national security, child protection, healthcare, and research purposes.

Justifications for processing

The conditions that organizations need to meet to keep collection and use of data on the right side of the law will be even tighter than they are now. For example, organizations will primarily be allowed to process only the minimal data necessary for the performance of a contract or legal obligation and for limited time with explicit consent. Even the rules for consent are expected to change radically with a clear and concise indication and acceptance for what purpose their personal data will be processed. No more silent, inactive consent or paragraphs of fine print in legal jargon that is not understood by the average person. Member states might be allowed to pass national legislation to fine-tune justifications in specific sectors such as employment and journalism.

Processors and supply chain

Exposure to data-related liabilities – for both customers and suppliers – will increase. With the regulation taking effect in 2018, new deals being negotiated now need to be future-proofed. Parties will need to document their data responsibilities even more clearly and the increased risk levels will impact negotiations on security standards, risk allocation and pricing.

[1] http://ec.europa.eu/priorities/digital-single-market/index_en.htm

Profiling

A data subject will have the right to object to decisions based on automated process, such as data profiling. However there are exceptions to this. For example, where an automated process is necessary to allow a contract to be performed or where automated processing is required by law, but it includes safeguards to protect an individual's rights. The outcome of this requirement needs careful consideration by advertisers, insurers, employers and other sectors which rely on the ability to profile individuals.

Consent and withdrawing consent (aka The right to be forgotten)

In order to protect EU citizens there is the need for them to consent to the use of their information. This isn't much different that most of the pieces of paper seen today, however there is a new wrinkle, the ability to withdraw consent. Data subjects' right to erasure of information (or withdrawing consent, formerly known as the right to be forgotten) will form a central part of the new GDPR. However these rights will not be absolute; for example data controllers will be required to perform a balancing act against any competing rights to freedom of expression when considering removal requests. Other exceptions, allowing for continued storage of data, are proposed.

For many organizations, the right to be forgotten will probably be the most challenging aspect of the GDPR. Apart from figuring out where the information is and how it can be deleted, there is also the need to ensure that other 3rd parties who you have shared the information with also comply with the request.

International transfers

While the new regime builds on the current framework with respect to the general principle for international transfers, the rules have been extended to apply to processors and to onward transfers of personal data to third countries or international organizations.

Security and breach notification

Data breach notification to the Data Protection Authority where a breach causes risks to individuals is now a requirement. This is an area where demonstrable management by organizations will be required and essential. Strict timelines and details have been established requiring organizations to notify the authorities in 24 hours and the specific individuals without undue delay. Notifications must include the nature, identity, recommended measures to prevent adverse effects and how the organization will address the breach.

The requirement for "appropriate" security will be extended to apply to processors as well as controllers, including demonstrating compliance with any applicable code of conduct (as yet to be defined) and the following:

- 'Pseudoanonymisation and encryption of personal data'
- 'The ability to ensure the ongoing confidentiality, integrity, availability and resilience of systems and services processing personal data',
- 'The ability to restore the availability and access to data in a timely manner in the event of a physical or technical incident',
- 'A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing'.

It is important to note that the GDPR is not simply a regulation to guide processes and best practices. The regulation clearly indicates and requires the appropriate and reasonable technical measures to be implemented to enforce policies and compliance.

Data Protection Officers

There is a new role required within the organization, the Data Protection Officer (DPO). Its primary function is to monitor the organization for compliance to the regulation ensuring the appropriate protection of the information which the organization holds. The rules and regulations around appointment of a DPO are relatively complex and it can be appointed to an individual outside the organization. For many this will be the case, especially for smaller organizations, as it will help resolve some of the internal conflict that could occur as the position needs to be seen as independent. "Don't shoot the messenger" will probably reverberate around offices in the months before the regulation comes into force as the DPO shows areas where improvement is needed.

The appointment of a DPO should not be a sticking point when it comes to planning for compliance. There is a lot of groundwork which needs to be done by the business and while a DPO could project manage and drive a compliance project, they are not essential at the start. A well-disciplined team from across the business is needed to drive progress towards compliance and prevarication is the greatest enemy to success.

Privacy by design

Controllers must implement appropriate technical and organizational measures and procedures to ensure that processing safeguards the rights of the data subject and that by default, only the minimum and necessary personal data for each specific purpose is processed and it is not disclosed more widely than necessary.

There is going to be a great deal written about the need for 'Privacy by design', but the reality is that there are thousands of applications out there where this was not considered. Unfortunately organizations can't start from a blank sheet of paper, legacy applications need to be included. For most, it will be technology that is required to monitor and block unauthorized information from the applications from leaving the organization. This needs to include the reports generated by the application as well as any other means that the information can be exfiltrated, for example through a web based interface.

How will the regulation work in practice?

Without the regulation being fully enacted there is a bit of guesswork here, but this is the way we think it will manifest itself.

Example 1

A multinational company with several establishments in EU Member States has an online navigation and mapping system across Europe. This system collects images of all private and public buildings, and may also take pictures of individuals.

With the current rules:

The data protection safeguards upon data controllers vary substantially from one Member State to another. In one Member State, the deployment of this service led to a major public and political outcry, and some aspects of it were considered to be unlawful. The company then offered additional guarantees and safeguards to the individuals residing in that Member State after negotiation with the competent DPA, however the company refused to commit to offer the same additional guarantees to individuals in other Member States.

Currently, data controllers operating across borders need to spend time and money (for legal advice, and to prepare the required forms or documents) to comply with different, and sometimes contradictory, obligations.

With the new rules:

The new rules will establish a single, pan-European law for data protection, replacing the current inconsistent patchwork of national laws. Any company – regardless of whether it is established in the EU or not – will have to apply EU data protection law should they wish to offer their services in the EU.

Example 2

A small advertising company wants to expand its activities from France to Germany.

With the current rules:

The company's data processing activities will be subject to a separate set of rules in Germany and the company will have to deal with a new regulator. The costs of obtaining legal advice and adjusting business models in order to enter this new market may be prohibitive. For example, some member states charge notification fees for processing data.

With the new rules:

The new data protection rules will scrap all separate notification obligations and the costs associated with these, replacing them with a single unified notification, consent and erasure processes which will need to be adhered to. The aim of the data protection regulation is to remove obstacles to cross-border trade.

Where to Begin

GDPR is not 'just' another regulation to be complied with. While global companies have had to comply with legislation from different countries and sectors, and in the majority of cases the basic purpose is the same – to protect critical information, GDPR has more stringent requirements including technical measures. However, GDPR will bring the need for compliance to organizations of all sizes and across all sectors, and the headline grabbing fines are creating stress in the boardroom. While that stress is not totally uncalled for, it is something that can be reduced by creating a plan.

First off, this is not just a problem for the CIO, or for the legal department, or the 'audit and compliance' group... this is something the whole business is going to need to be involved in. There is a need for a cross functional team who can get to grips with what needs to be done and then make it happen.

GDPR is about information. Information collection, analysis, storage and sharing. So the place to begin is to understand what information you have which would fall under the GDPR. Once you understand this, then the next step is to understand its processing purpose of which you have consent, define where it is stored, how it flows within the organization and outside it, and who has access to it.

Armed with information about your information, a plan for compliance can be drawn up. Where is the greatest risk and how will you address it?

How Clearswift Can Help

The primary goal of GDPR is to protect EU citizens critical personal information. It is important to put an education and awareness program into place as to why GDPR is important and the consequences of getting it wrong. This needs to be coupled with corporate information polices to protect the information, however, it is technology which must be used to enforce the policy and protect both the employee as well as the organization.

Clearswift helps global organizations comply with GDPR with an unprecedented level of real-time data visibility, intelligent policy enforcement and adaptive security. Clearswift products can be used to help drive towards compliance and the ongoing monitoring and enforcement.

Data Visibility

You can't protect want you can't see. Discover personal data distributed and hidden on servers, desktops/notebooks, and network shares, while inspecting information before it leaves your organization through email, web, social media and cloud storage and collaboration apps.

Gaining such visiblility into your data can initially be used as part of a privacy audit, assessing how great the problem of control might be, or at a later point in time, as part of a Data Protection Impact Assessment which needs to happen if specific events occur which might infringe on the rights of EU citizens. However, it can also be used as part of a 'right to be forgotten' request where discovery of the information held in unstructured files on endpoints and file servers is needed. The action of deletion can then be carried out automatically or manually.

Intelligent Policy Enforcement

Not all data, access and sharing rights are created equal. Intelligent polices can be applied consistently across all channels and based on GDPR geo, data type (i.e. national security, child protection, healthcare, etc.), purpose conditions and required security treatment.

Intelligent policy enforcement uses both context as well as content in making policy decisions. The context is the sender and the recipient (or target upload site) as well as the communication mechanism, for example email, web or endpoint. A single shared policy creates consistency as well as easy of deployment and use. A document might be sent by corporate email and the policy action would be to encrypt the communication. However the same file might be uploaded to a cloud collaboration site, in which case the action could be to redact the sensitive information. Finally, the same user might want to copy it to a USB stick, at which point the system can block it.

Adaptive Security

Protecting the egress points is critical to protecting GDPR information from losses or leaks through accidental insider mistakes, the malicious insider or malevolent external attacks.

Adaptive security applied in real-time based on specific GDPR policy, whether it calls for automated redaction, encryption, blocking, moving or deleting. Clearswift's unique Adaptive Redaction technology makes GDPR enforcement a reality for most organizations by removing only the required personal data from being shared, allowing the rest of the digital activity to continue without business disruption and false positives. Complete protection that goes unnoticed from the end user.

Governance

Whether you are the Data Protection Officer (DPO), compliance manager or IT security professional, you will be provided complete visibility into reports, policy violations, quarantined data, logs, etc. Clearswift's unique track and trace capability not only enables real-time policy and adaptive security enforcement, but enables violation/breach analysis to identify loss of personal data, sources and exposure required for notifications.

Additionally, the granular tracking of information at a file and a sub-file (information) level helps GDPR to monitor information across the organization boundary to 3rd parties. Information provenance reports can be used to determine which information has been sent to which 3rd party, so the correct organizations can be chased in the event of a 'right to be forgotten' request being enacted.

Clearswift and the European Union Nations

Our regional expertise and unique relationships with EU governments provide our solutions the alignment and insight required to help global organizations stay in compliance with GDPR.

Effective GDPR compliance relies upon the solutions enforcing policy being able to adapt to the needs of the organization. Not just today, but in the future as well.

Summary

The General Data Protection Regulations, or GDPR, are on their way. At the time of writing, enactment is less than two years away. For IT projects this is a very short timeframe, and while this is not just about IT, IT is a significant part of the project – which will undoubtedly need budget. Budget cycles tend to happen once per year, particularly for larger ones, which means that unless you have already made provision in this year's budget, there is only one more cycle before the regulations go live. A scary thought.

GDPR should be seen as an opportunity to get your information management and governance in order. In the same way that Y2K was seen as a project to get your systems in order, GDPR is about getting your information in order. For many, this will be the first time that they really understand the information in their organization and put any real controls around it – protecting it wherever it may be.

The process of compliance begins with understanding the information, building the appropriate corporate polices around how it should be protected and then enforcing those policies through the use of technology.

GDPR is not just about the largest global companies, it is about any company in any sector who does business in the EU. As such, the technology solutions which can be used to help gain compliance need to be focused on ease of use for all to use.

Clearswift provides solutions to help with the initial understanding of your information and the protection, management and governance of that information moving forwards.

clearswift

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 **www.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