Getting Started on the Basics: The EU General Data Protection Regulation (GDPR)

The May 2018 GDPR enforcement date is rapidly approaching. Given the magnitude of potential fines, new rights for individuals to claim compensation, and the prevalence and effectiveness of cybercrime, a GDPR breach plan should go straight into every organisation's (and Corporate Board member's) risk register.

Introduction

The current data protection framework in the European Union (EU) is governed by the 1995 European Directive on the protection of individuals with regard to the processing of personal data (the **Directive**), which Member States had to implement into their own national legislation. Due to differences of interpretation, the Directive has been implemented differently by EU Member States into their national laws, resulting in an inconsistent patchwork of data protection rules within the EU.

In order to simplify the rules to be applied throughout the EU, a new EU data protection framework has been adopted in the form of a regulation: the General Data Protection Regulation (GDPR). As it is an EU regulation, there will be no need for EU Member States to adopt additional legislation to make the rules applicable in their national system. Instead, the regulation will automatically apply to all EU countries. However, there will still be some areas where EU Member States are permitted to legislate (differently) within their national system (e.g. in relation to the processing of employee data); and, there will undoubtedly still be some variation in applicable data protection rules among the EU Member States.

GDPR forces a company-wide strategy on managing the information lifecycle as opposed to a tick-the-box compliance approach. Unfortunately, there is no one-size-fits-all GDPR compliance plan and the amount of work required will vary depending on your organisation and its current data practices and processes. You may need, for example, to implement new procedures to deal with GDPR's new "privacy by design" requirement or new provisions on transparency and individuals' rights. These are requirements likely to need institutionalization of new ideas, and behaviors as well as preparedness for the incorporation of new measures.

It is therefore crucial for executives, employees and managers to understand how addressing GDPR requirements may impact operational practices at every level. Operations managers would need to determine what personal data they are currently storing, where it lives, how it flows within the organization, how it is shared, how it is secured and whether third parties will need to access it. For example, in a large or complex organisation, preparing for GDPR may have significant budgetary, IT, personnel, governance and communications implications and may require additional time and resources for implementation.

GDPR places greater emphasis on the documentation that data controllers (which are those who determine when, how and for what purpose personal data is to be processed) must keep to demonstrate their accountability. Compliance will require organisations to review their current approach to governance and analyse how they actually manage data protection as a corporate issue. One aspect of this might be to review the contracts and other arrangements in place when sharing data with other organisations (including cloud services agreements and outsourcing). It is essential to start planning, as early as you can,

and to gain 'buy-in' from key stakeholders in your organisation. Here we offer an overview of the key areas to be addressed to help them understand the task ahead.

The Basic Considerations for all Organisations

- **The penalties for violations have become much more severe.**

Under the current data protection framework, the Directive left to the EU Member States the discretion to decide the maximum level of fines to be imposed. This resulted in strong discrepancies between the EU Member States: fines may amount to EUR 25,000 in Austria, EUR 150,000 in France, EUR 600,000 in Spain or £ 500,000 in the United Kingdom. In a number of matters involving privacy violations, data protection authorities (**DPAs**) had little recourse against large, well-funded multinationals who could be tempted to view such fines as merely the "cost of doing business".

Under Article 83(5) of t GDPR, DPAs would be able to impose fines of up to €20M or 4% of the offending company's total worldwide annual turnover of the preceding financial year, whichever is higher.

In addition, individuals may also seek to enforce their data protection rights: Article 82(1) of the GDPR provides that any person having suffered material or non-material damages as a result of the processing of his personal data may claim for compensation.

- **The definition of what is considered "personal data" has increased in scope**

Under GDPR, the definition of "personal data" will cover a wider range of data types. Article 4(1) provides that:

> *'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.*

It has been made clear within GDPR (recital 30) that IP addresses, cookie identifiers, mobile device ID and other types of online identifiers are deemed to be "personal data" and must be protected accordingly.

- **GDPR has a wider geographical scope**

Article 3 of the GDPR provides that the new rules apply to entities established in the EU and the Economic Exclusive Zone (EEZ) that are processing personal data either for their own purposes (as "data controllers") or on behalf of another entity (as "data processors"), regardless of whether the processing of data actually takes place in the EU or not. Shipping vessels that work within the EEZ are included for example. In addition, Article 3(2) further provides that GDPR will apply worldwide to any processing of personal data of individuals who are in the EU, whenever such processing is related to the offering of goods or services (including those that are free) to individuals in the EU, or where the behaviour of EU individuals is monitored.

In practical terms, this means that any company that does business with EU residents (e.g. marketing of goods or services) will be subject to GDPR, even if they operate outside of the EU and do not have

any premises or equipment in the EU. Anyone operating a website accessible from the EU (which could be considered the provision of a free electronic service) may be subject to GDPR, and as described in the above point, the collection of IP addresses in access logs, or the tracking of visitors using cookies, JavaScript or other tracking technologies would trigger the application of GDPR.

- **A data processing register is mandatory**

Article 30(1) of GDPR requires data controllers and processors to maintain a written record (which may be in electronic form) of processing activities under its responsibility, while Article 30(4) further provides that such record must be available to the relevant DPA upon request.
The record must include the following:

- the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;
- the purposes of the processing;
- a description of the categories of data subjects and of the categories of personal data;
- the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;
- where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and the documentation of suitable safeguards;
- where possible, the envisaged time limits for erasure of the different categories of data;
- where possible, a general description of the technical and organisational security measures in place to safeguard the data.

If the above requirements are not met, Article 83 (4) of GDPR provides that an administrative fine of up to EUR 10 Million or 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

The regulation states that the record requirement does not apply to small organisations (less than 250 people, however we can expect many small and medium size organisations will be required to maintain and keep the records if:

- the processing is likely to result in a risk to the rights of affected employees (e.g. scoring, comprehensive monitoring, high risk resulting out of unauthorized disclosure or access, use of new technologies);
- the processing is not occasional; or
- the processing includes special categories of data as outlined in Article 9 (1) (e.g. health data, biometric data, data related to political or philosophical beliefs) or personal data relating to criminal convictions and offences referred to in Article 10 of GDPR.

- **New user rights have to be implemented**

  As detailed in Articles 13-22, organisations will need to ensure that effective systems and processes are in place to give effect to the following rights:

  1. The right to be informed
  2. The right of access

3. The right to rectification
4. The right to erasure (the 'right to be forgotten')
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

Organisations will need, for example, to have a policy in place to determine when certain data is no longer necessary to retain; for how individuals will be able to withdraw their consent; and to deal with user requests when they object to the processing of their data.

Given how often enterprise data is simply archived rather than deleted and the sheer volume of such data, removing irrelevant personal data on request is undoubtedly going to be a big challenge. Server and device logging, which can capture a substantial amount of personal data by itself, will likely be a target for erasure requests.

- **Technical and organisational [security] measures are mandatory**

GDPR requires data "controllers" (which are those who determine when, how and for what purpose personal data is to be processed) to "implement appropriate technical and organizational measures" to protect the personal data that they hold and the risks that are presented in the processing of the data, "*in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.*"

Article 32 also provides certain examples of the security measures expected:

- the pseudonymisation (e.g. hashing) and encryption of personal data,
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal 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 organisational measures for ensuring the security of the processing.

- **Data protection impact assessments are now required**

Data protection must now be designed into systems by default and privacy impact assessments (PIAs) – or what the GDPR calls data protection impact assessments (DPIAs) – are now mandatory (Article 35) for technologies and processes that are likely to result in a high risk to the rights of individuals (e.g. profiling leading to decisions that produce legal effects for the individual or processing on a large scale). The DPA may list specific situations for which a DPIA is or is not required, while most organisations should, as part of their privacy-by-design and default strategies, ensure that a DPIA is now part of their risk assessment process.

- **Personal data breaches must be reported**

It will become mandatory (Article 33 of the GDPR) for an organisation to report any data breach to its DPA within 72 hours of becoming aware of it. If that requirement is not met, the eventual report must be accompanied by an explanation for the delay. The notification must follow a specific format, which includes a requirement to describe the measures being taken to address the breach and mitigate its possible side effects.

Where the breach may result in a high risk to the rights and freedoms of individuals, they must be contacted "without undue delay after becoming aware of" the data breach. This communication will not be necessary if appropriate protective measures – such as encryption – are in place to eliminate any danger to the affected individuals.

- **A Data Protection Officer is required for certain organisations**

In certain circumstances, an organisation may be required to designate a Data Protection Officer (the **DPO**), i.e. where the "core activities" of the organisation involve the monitoring of individuals on a large scale or where there is a large scale processing of "special categories of data" (e.g. an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data if processed in order to uniquely identify a natural person, health, sex life or sexual orientation).

Summary

While the GDPR is not yet applicable, its enforcement date is rapidly approaching and it is necessary to use the remaining time left to prepare for the new requirements. The scope of the requirements is broad: GDPR forces a company-wide strategy and review of processes for managing personal data on every level, and it includes various types of online data in its definition of personal. New rights and obligations must be accounted for and every organisation will have to work out its own approach to reflect the context and practices of the business. It is crucial that the management of the GDPR compliance plan becomes a top priority on the agendas of the board and top management.

This document was prepared by members of the (ISC)^2 EMEA Advisory Council GDPR Task Force. Lead Contributors: Yves Le Roux, CISSP, CISM; Paul Lanois, CCSK, CIPM, CIPT, CIPP (A, E, US and C), FIP, CISMP and LLM.

Reviewed by Dr. Adrian Davis, MBA, FBCS CITP, CISSP; Sam Berger, CISSP; Michael Christensen, CISSP, CSSLP, CISM, CRISC, CIS LI, EU-GDPR-P; CCM, CCSK, CPSA, ISTQB, PRINCE2, ITIL, COBIT5; Ramon Codina, CISSP; Santosh Krishna Putchala, CISSP