Your GDPR Journey

Business made better

MASON HAYES & CURRAN

Saros

Introduction

The European Union's new General Data Protection Regulation[1] will come into effect on the 25th of May, 2018. The GDPR marks a significant change in the EU data protection and privacy regime. It will repeal and replace the current EU Data Protection Directive[2], which forms the basis for the existing data protection regimes in Ireland, the UK and across Europe. Grounded in industry experience, it is the remit of this paper to provide a pragmatic approach to help put your organisation on the road to compliance with the GDPR.

The GDPR marks a significant change in the EU data protection regime. It will repeal and replace the current EU Data Protection Directive, Directive 95/46/EC, which forms the basis for the existing data protection regimes in Ireland, the UK and across Europe.

The scope and standards of the GDPR reach wider and higher than its predecessor.

The GDPR applies both to organisations established in the EU and to non–EU established organisations that target or monitor EU residents.

It introduces the principle of accountability, which means that affected organisations will have to work on their internal compliance.

New requirements relating to consent, breach notification, transparency, and the appointment of data protection officers **(DPOs)** mean impacted organisations need to revise their policies and operations procedures.

These changes are important due to significant penalties and fines for non-compliance of up to €20 million or 4% of annual revenue. The purpose of this paper is to guide organisations through the practical steps required to become GDPR compliant.

Approach

This article outlines a methodology that an organisation can follow to help it become GDPR compliant.

This methodology has four phases:

1. *Assessment* - results in an understanding of an organisation's current data-related environment
2. *Gap Analysis* - compares an organisation's current data-related environment with the GDPR
3. *Remediation* - progresses the Assessment Phase / Gap Analysis to the execution of activities needed to reach compliance.
4. *Adherence* - specifies the actions necessary to maintain and update compliance.

1. Assessment – *where you are*

The first step involves an assessment of your organisation's information processes and procedures from the ground up.

Data protection compliance should be embedded within the DNA of an organisation, in all of its processes, products and services.

Your assessment should involve a variety of components related to your organisation's activities, including but not limited to hardware, security, software, contracts, policies and paperwork and training.

Upon completion of the assessment phase, all findings should be documented.

Hardware

As part of the assessment you should examine the hardware your organisation uses to process data to determine its capability to maintain appropriate security and confidentiality in respect of personal data.

This will involve considering the nature of the personal data and the costs and practicalities of implementation and rectification.

Security

You will need to evaluate the security risks inherent in your organisation's processing of data and assess its current ability to manage and mitigate those risks.

In assessing data security risks, you may wish to consider the information security and data protection risks of processing personal data, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage.

Software

You should review the software involved in your organisation's data processing activities to assess what types of personal data it captures and what controls are in place in respect of managing this data capture.

It is important to identify whether this data is being disclosed to third parties outside the European Economic Area as a different legal standard will apply to each depending on the destination.

Contract Analysis

The GDPR requires parties to include appropriate data protection language into all contracts that involve the processing of personal data.

Many day-to-day commercial and IT contracts that an organisation enters into will involve some form of data processing. Examples include services agreements, sourcing agreements, consultancy agreements, and cloud contracts.

You should identify all contracts that relate to or are connected with the processing of personal data.

Where your organisation is acting as the capacity of a data processor, it will also need to assess all contracts with its sub-contractors (known in this context as 'sub-processors'), as the GDPR requires the organisation obtains the written authorisation of the controller.

Policies and Paperwork

You will need to assess your organisation's current privacy notices and policies as they are unlikely to provide for the higher thresholds under the GDPR regarding valid consents or methods for communicating to relevant individuals.

This should be undertaken as part of a full review of all of your current privacy compliance paperwork in light of the expansion of data subjects' rights under GDPR.

Consent

Today, organisations commonly justify processing based on an individual's consent or on the pursuance of legitimate interests of that organisation. The GDPR changes both of these standards.

Under the GDPR, consent must now be in the form of an unambiguous indication of the individual's wishes by a statement or clear affirmative action, for example, ticking a box, choosing technical settings on a website, or a signature.

You should also carefully review all consents your organisation obtained prior to the GDPR coming into force. If these consents were not given in line with the requirements of the GDPR, they will no longer be valid and new consents will need to be secured.

Training

Your organisation will also need to assess the adequacy of data protection training provided to employees and contractors involved in data processing activities.

2. Gap Analysis – *which shortfalls exist*

The Gap Analysis follows the Assessment Phase and is a comparative study between an organisations current data-related environment versus the future compliant environment as set forth by the GDPR. It establishes the delta between the two states.

The Gap Analysis reveals if the organisation is compliant and acts as an enabler for future remediation activities. In the current context, an organisation's data-related environment, i.e. the results of the assessment phase, is to be compared to the GDPR.

Prior to completing a Gap Analysis, it is important that an organisation has a firm understanding of the topics and areas covered under the GDPR.

A three-step process may be employed when conducting a Gap Analysis:

1. *Analyse the organisation's current situation*
2. *Identify the desired future state of compliance the organisation wishes to reach, i.e. with the GDPR*
3. *Define the delta between steps 1 and 2*

Upon completion of the above steps, it can be determined whether or not the organisation is GDPR compliant. If a requirement of the GDPR is not being met, a gap exists which requires remediation. The remediation is the implementation of the missing requirement(s).

3. Remediation – *what you need to do*

Once you have identified gaps in your compliance with current EU law and the GDPR from your assessment, it is time to take compliance and corrective actions.

The GDPR will require some organisations to appoint a DPO where the core activities of an organisation consist of processing data through regularly monitoring individuals on a large scale. A DPO will ensure an organisation is aware of, and complies with, its data protection responsibilities.

Remediation involves the creation of an action plan that will bridge the documented gaps. This plan facilitates moving from a state of non-compliance with the GDPR, to a compliant environment.

An organisation should promptly rectify deficiencies revealed from the assessment of data-related matters. Possible actions include hardware upgrades, data storage projects, and improvements to software security.

Software

Your organisation may need to adapt its software and systems to enable it to capture your end users consent that they provide by clear affirmative action, such as box ticking. Your software and systems must facilitate the individual's right to withdraw consent or to object to processing on the grounds of legitimate interest.

Security

Security measures specified under the GDPR can be integrated into the processing system, such as encryption or pseudonymisation of data.

Your organisation may need to amend its security protocol to minimise the processing of personal data, increase transparency with regard to the processing of personal data and enable the controller to create and improve security features.

With respect to notification rules, template security breach notifications and security breach response plans should be prepared to ensure compliance with notification rules.

Contracts and Policies

Organisations can take action in respect of their contracting by preparing template processing and sub-processing agreement provisions to cover the GDPR's expanded requirements in respect of security and breach notification.

Many of your existing contracts may need to be renegotiated to accommodate the GDPR's expanded requirements, so work needs to start now with your legal advisers.

Drafting or amending of organisations' compliance suite of documentation can begin with respect to data breach register, data governance records and privacy impact assessments.

Subject access request handling policies will also need to be updated to reflect the expanded categories of information to be provided to individuals and reduced response times in which to do so.

Training

Personnel training on data protection should be updated in order to familiarise employees with security protocol and notification obligations.

4. Adherence – *where you need to be*

Once you have taken the required action to reach the desired destination of GDPR compliance for your organisation, the final step is maintaining this status.

This will require on-going continued efforts on the part of an organisation and it's DPO, if one is appointed.

Any new business initiatives should be reviewed and their impact assessed to ensure ongoing compliance with the GDPR.

Compliant organisations will require sustained engagement and monitoring from legal, regulatory and IT perspectives to ensure that current and future data-related activities meet GDPR standards.

The one-stop-shop mechanism implemented by the GDPR means that organisations will be subject to a single supervisory authority, even where they have a number of establishments across the EU. Each supervisory authority has the power to carry out investigations in the form of data protection audits. They may access any premises and review any data processing equipment and means, thus rendering on-going GDPR compliance as critical.

Organisations that control personal data are required to maintain a record of any personal data breaches to enable the supervisory authority to verify compliance with the controller's notification obligation.

The GDPR introduces new concepts of privacy by design and privacy by default.

Privacy by design requires organisations to consider privacy measures during the embryonic stages of the product design processes.

Privacy by default requires data controllers to ensure that, by default, only necessary data is processed.

To make sure that organisations are able to maintain their data protection obligations, these concepts should be incorporated into the D.N.A. of an organisation, throughout the development, design, selection and use of applications, services and products.

Where to from here?

The GDPR will have a tangible impact upon European organisations when it comes into effect on 25th May 2018.

The road to compliance will involve the implementation of, and continuous adherence to, a purposeful methodology.

While this paper outlines what needs to be done from legal, regulatory and IT perspectives, compliance with GDPR will not be a box ticking exercise, and will only be achieved by working with experienced professional advisers to arrive at and maintain GDPR compliance.

If you have any queries in relation to this article or would like to know more about the GDPR, please contact the authors below.

Ray Armstrong
CEO
t: +353 1 653 3171
m: +353 87 601 4405
e: ray.armstrong@sarosconsulting.com

Ray is currently CEO of Saros. Ray has over 15 years' international IT experience in varying industries including pharma, medical device, manufacturing and professional services. He is an innovative, adaptable international IT executive with a highly effective mix of IT and business skills. His expertise is in IT strategy and programme management. Ray has gained considerable experience in the development, deployment and management of mission critical international IT environments.

Jeffrey Hughes
IT Strategy Consultant
t: +353 1 653 3171
m: +353 87 176 9505
e: jeffrey.hughes@sarosconsulting.com

Jeffrey is an IT Strategy Consultant at Saros. He holds a Ph.D. in Strategy and IT from Trinity College Dublin. At Saros, Jeffrey's expertise resides in advisory and compliance services pertaining to IT strategy, in addition to being a certified PRINCE2 Practitioner in project management. The EU's upcoming General Data Protection Regulation (GDPR) and the Central Bank's IT and Cybersecurity guidelines represent particular areas of focus.

Mark Adair
Senior Associate
t: +353 1 614 2345
e: madair@mhc.ie

Mark is a senior associate on the Commercial law practice group at Mason Hayes & Curran in Dublin. Mark advises clients such as Facebook, Ladbrokes and Core Media on a broad range of complex technology matters. He has a particular focus on the areas of data protection, fintech and cloud computing.

Áine Hogan
Trainee Solicitor
t: +353 1 614 2166
e: ahogan@mhc.ie

Áine is a trainee solicitor due to qualify this year as an associate. She is working on the Commercial law practice group at Mason Hayes & Curran in Dublin. She assists on data protection, privacy and IP matters, as well as commercial contracts.