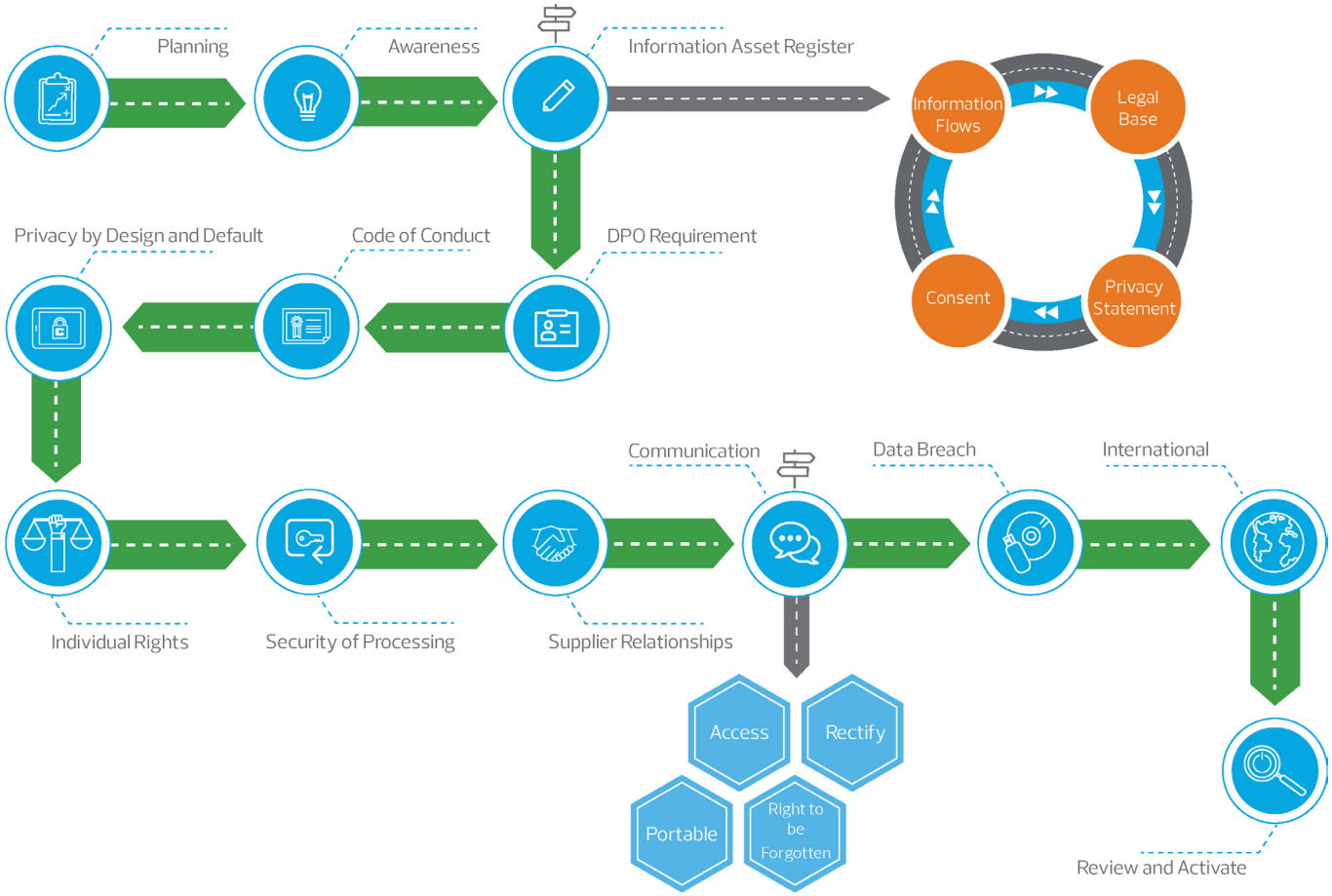
GDPR ROADMAP TO COMPLIANCE



In light of the rapid advancements of the digital age, GDPR is intended to strengthen data protection for all individuals within the EU. The reforms have fundamentally changed the way organisations store, share, process and protect the personal information of customers, clients and employees. It impacts all organisations within the EU including those who transfer personal data of EU citizens across borders within the EU.

RSM uses the following process to help organisations comply with the GDPR.

PLANNING

Organisations require a project team to represent all functions in planning and implementing the GDPR. The project team will vary according to the size of the organisation but may be comprised of 'Heads of Functions'. With severe fines of up to 4% of global revenue or €20 million (whichever is greater), senior decision makers should be fully informed about the impact of GDPR on the business.

AWARENESS

A comprehensive breakdown of GDPR requirements should be communicated to both the management and staff of the entire organisation through hosted training seminars, webinars or internal awareness campaigns that will help to educate individuals and raise awareness about the impending changes to the company's policies and procedures.

INFORMATION ASSET REGISTER

The GDPR requires that businesses will need to evidence how they process the personal identifiable information it holds, from collection to disposal. A simple way to identify and manage an organisation's information assets and their associated risks is with an Information Asset Register which provides a catalogue of information held, where it is stored, how it moves and who it is shared with. Identifying the data allows it to be assigned a classification and the necessary protection reflecting this.

DPO REQUIREMENT

A Data Protection Officer (DPO) is an enterprise security leadership role – they are responsible for overseeing the data protection strategy and implementation to ensure compliance with GDPR requirements. The DPO role differs from the Chief Information Officer (CIO) and Chief Information Security Officer (CISO) roles. The GDPR requires the appointment of a DPO in three cases;

- If processing is carried out by a public authority (except courts)
- In private companies where the 'core activities' consist of processing operations which require 'regular and systematic monitoring' of data subjects 'on a large scale'
- In 'large scale' processing of sensitive data or data relating to criminal convictions and offences

CODE OF CONDUCT

An organisation should develop a code of conduct and certification mechanisms to demonstrate its compliance with the GDPR. The code of conduct should be visible and accessible online. There are a number of benefits to having a code of conduct; these include increasing transparency and accountability, providing mitigation against enforcement action and improving standards by establishing best practice.

PRIVACY BY DESIGN

Under the new regulation, high risk privacy data which affects an individual's rights should be evaluated at the start of the project. The method to test this is called a data protection impact assessment (DPIA). This is a potential approach to the GDPR that will help organisations to comply. Privacy and its considerations cannot be ensured simply by legislation alone; it should be a fundamental component that is integrated into project risk management, methodologies and policies. The data processor and/or controller is required to implement appropriate technical measures to ensure data protection principles are met.

INDIVIDUAL RIGHTS

Under the GDPR, individuals must give consent in an active, free and unambiguous manner. This means that the use of 'opt-outs' is no longer permissible on websites and under the new regulation, individuals must 'opt-in', i.e. their choice must be explicit. Other significant changes include the right to be forgotten and the right to data portability. Organisations should review their ability to manage these rights.

SECURITY OF PROCESSING

Data security measures should, at a minimum, allow:

- Pseudonymising or encrypting personal data.
- Maintaining ongoing confidentiality, integrity, availability, access and resilience of processing systems and services.
- Restoring the availability and access to personal data in the event of a physical or technical security breach.
- Testing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing, including Privacy Impact Assessments (PIAs).

SUPPLIER RELATIONSHIPS

The GDPR creates clear lines of accountability over data processing, especially when it comes to defining the responsibilities of the 'data controller' and the 'data processor'.

An organisation, or the party determining the purpose and means of processing, are deemed to be the 'data controllers'. Their third-party suppliers who process personal data on behalf of the controller would be referred to as 'data processors'. The burden for personal data protection will primarily lie with data controllers.

Contracts with data processors should be reviewed and amended to ensure they meet the GDPR requirements, regardless of where the data processor is located.

COMMUNICATION

The GDPR requires more consistent and comprehensive protection of personal data which puts individuals and their rights at the heart of the reforms. The right of access, the right to be forgotten, the right to data portability and the right to object are just some of the changes encapsulated in the regulations. Organisations have a duty to communicate data subject rights.

DATA BREACH

In line with the accountability tenet of the GDPR, an organisation should develop or update their internal breach notification procedures and processes. If there is a data breach which presents a risk to the rights and freedoms of an individual, the organisation has 72 hours to report it. Data Protection Officers and key personnel should be involved in developing these procedures which will consider measures to mitigate the adverse effects of any breach. In addition, an organisation should keep a record of information security incidents. This includes evaluations of any data leaks, as well as recording the decision to report the incident to the Information Commissioner's Office (ICO) and /or to the individuals.

INTERNATIONAL

International organisations should make sure that processes and procedures are in place when data is being stored, processed or shared across EU-borders. The provisions of the GDPR must be applied to ensure that the protection of individuals guaranteed by the regulations are not undermined.

REVIEW & ACTIVATE

Organisations have between now and 25 May 2018 to prepare for the GDPR and ensure they adhere to the reforms. This time should be used to plan policies and procedures that manage and demonstrate compliance. All aspects of the GDPR should be communicated and understood by all individuals within the organisation.

For more information on how RSM can help, please contact
Terry: tmcadam@rsmireland.ie