WAVESTONE

# HOW TO ADDRESS THE MAJOR GDPR IMPLICATIONS - OUR KEY GUIDELINES

THE GENERAL DATA PROTECTION REGULATION (GDPR), WHICH COMES INTO FORCE ON 25TH MAY 2018, WILL SIGNIFICANTLY CHANGE THE WAY ORGANISATIONS OPERATE AND DEAL WITH DATA. NON-COMPLIANCE COULD LEAD TO SIGNIFICANT FINANCIAL PENALTIES OF UP TO 4% OF GLOBAL ANNUAL TURNOVER. THIS IS CRITICAL WHEN ONE CONSIDERS THAT CURRENT LEGACY SECURITY SYSTEMS AND DATA HANDLING PRACTICES ARE BOTH A NON-COMPLIANCE AND A CYBER SECURITY RISK FOR MOST ORGANISATIONS. PROACTIVE ORGANISATIONS ARE ALREADY TAKING MEASURES TO RE-EVALUATE AND TRANSFORM THEIR DATA PROTECTION AND PRIVACY AGENDA TO PREPARE FOR GDPR COMPLIANCE. IN THIS INSIGHT, WE IDENTIFY THE MAJOR IMPLICATIONS OF GDPR AND PROVIDE KEY GUIDELINES TO ACHIEVE COMPLIANCE.

INSIGHTS

# HOW TO ADDRESS THE MAJOR GDPR IMPLICATIONS

## 1 IMPLICATIONS OF GDPR

GDPR applies to organisations/ businesses of all sizes and sectors and to business activities established within the EU or even outside the EU (if trading with the EU). The implications with significant impact include the following:

### 1.1 ACCOUNTABILITY

Organisations will need to work at three different areas of data accountability:

- Transparency – by publishing accessible and easy to understand information and communication relating to the processing of personal data
- Traceability – by maintaining records of processing activities
- Cooperation with authorities – by providing any information or documents required.

The person responsible for ensuring accountability will be the Data Protection Officer (DPO), which will become a mandatory role for most companies.

### 1.2 PRIVACY BY DESIGN

What this means in practice is that organisations should:

- Integrate data protection as a key requirement at the beginning of every project
- Find the appropriate balance between the volume of collected data and the purpose for which it is processed
- Perform a 'Privacy Impact Assessment' to identify and reduce privacy risks of projects
- Adopt adequate security measures in order to mitigate the identified risks, considering the risks for privacy linked to the particular types of data processing.

### 1.3 DATA BREACH NOTIFICATION

The data controller (i.e. the company) will be obliged to notify any data breach, without undue delay, to:

- The supervisory authority (i.e. the Information Commissioner's Office), unless the personal data breach is unlikely to result in a risk to the rights and freedoms of individuals
- The data subject (i.e. the customer/ partner/ employee to whom the data relates), when the personal data breach is likely to result in a high risk to their rights and freedoms.

### 1.4 RIGHT TO ERASURE

The data controller shall erase personal data without undue delay when:

- Data are no longer necessary regarding the purposes for which they were collected or processed
- The data subject withdraws consent or objects to the processing of personal data
- Data have been unlawfully processed
- Data have to be erased for compliance with a legal obligation.

## 2 KEY GUIDELINES TO ADDRESS THE GDPR IMPLICATIONS

To address these implications and achieve GDPR compliance, organisations need to start preparing now. Following are our key guidelines and actions on how to prepare for GDPR compliance:

### 2.1 ESTABLISH ACCOUNTABILITY

- Appoint a Data Protection Officer (DPO) who has the overall responsibility for data accountability
- Design and implement processes to trace, control and report on data usage (e.g. with applicative logs / Security Information and Event Management (SIEM) or Identity and Access Management (IAM) initiatives).

### 2.2 IMPLEMENT 'PRIVACY BY DESIGN'

- Update existing processes and templates to include the data privacy dimension for all new projects – develop repeatable framework documents
- Develop a pragmatic Privacy Impact Assessment (PIA) framework and perform PIA for all projects/services to prioritise the most sensitive ones
- When starting a new project, integrate data privacy measures at all stages of the project from the beginning, rather than introducing them at the end
- For existing data treatment, focus of improvement should be on processes that handle the most sensitive data.

### 2.3 ESTABLISH DATA BREACH NOTIFICATION PROCESSES

Organisations will have to notify the relevant parties within 72 hours of becoming aware of the data breach. To bring this into practice:

- Adapt existing crisis management frameworks to include data breach notification and data leakage management processes
- Conduct frequent exercises involving all stakeholders to test the effectiveness of crisis management plans to deal with similar/ real life events.

### 2.4 IMPLEMENT SYSTEMS AND PROCESSES FOR 'RIGHT TO ERASURE'

- Define guidelines on data conservation periods
- Identify and maintain documentation logs of

existing data (location/ need for conservation/ deletion)
- Implement the data privacy user-request management process, including deletion request.

## 3 CONCLUSION

The period granted for GDPR enforcement, with a deadline for full regulatory compliance by 25th May 2018, is a challenging implementation timeframe. This issue should not be overlooked, considering the increasing media exposure (Google on the right to be forgotten, Facebook on the informed consent of Internet users) and the severity of the financial penalties resulting from non-compliance. Achieving early GDPR compliance is an opportunity to enhance your organisation's credibility in the eyes of customers and the regulator. We strongly advise to start enforcing this regulation as soon as possible by creating work-streams to implement the key guidelines highlighted in this insight.

## ABOUT US

Wavestone is an international consultancy that provides connected thinking, insight and capability to industry leading organisations. We work collaboratively with our clients to plan strategic business transformation and seamlessly turn strategy into action.

## FIND OUT MORE

If you'd like to find out more, please contact us by calling at +44 20 7947 4176, or via email at **enquiries@wavestone-advisors.com** or visit our website at **www.wavestone-advisors.com**

WAVESTONE

www.wavestone-advisors.com