INTRODUCTION

A framework for Airmic members

EU member states are entering the final countdown to the EU General Data Protection Regulations (GDPR), which apply from 25th May 2018 and bring with them a huge change in data protection law.

All organisations should already be familiar with the main provisions of the GDPR (Full details are provided in *The EU General Data Protection Regulations: What risk managers need to know, Airmic 2017*). However, many are now asking themselves how the GDPR applies to them and what they need to do in practical terms to ensure compliance in time.

The GDPR seek to balance the privacy rights of individuals with the capacity of businesses to use data for their own purposes in the internet era. It can be tempting to leave compliance to the IT team. However, GDPR concerns far more than information security and is a business-wide issue which requires a complete change in business culture. Whether or not an organisation appoints a data protection officer, risk managers will remain key to ensuring that the risk of non-compliance is properly understood across the organisation.

Complying with GDPR is not a one-off project. An integrated, thorough and transformational programme is required that addresses how an organisation's personnel, processes and systems handle personal data. Taking a step-by -step approach can make this challenge more manageable.

> "THESE SWEEPING REGULATIONS CAN BE OVERWHELMING. WE ARE BREAKING THEM UP, COMPARTMENTALISING AND TAKING BITE-SIZED ACTIONS. OTHERWISE IT'S FAR TOO EASY TO FALL DOWN THE GDPR RABBIT HOLE!"
>
> SCOTT WILSON, CHIEF INFORMATION SECURITY OFFICER, VENTIV TECHNOLOGY

- Organisations must have a comprehensive GDPR implementation programme which is mandated by the Board and effectively implemented at management level
- Individuals within organisations must fully understand and perform their data protection obligations and responsibilities
- Organisations must be able to produce clear evidence to demonstrate with that they comply with the GDPR
- This paper provides a practical step-by-step framework for organisations when navigating the major risks posed by the GDPR.

A REMINDER: MAJOR PROVISIONS

1. **Mandatory reporting** of data breaches within 72 hours
2. **Hefty fines**, of up to 4% of annual global turnover or €20 million
3. **Appointment of a data protection officer (DPO)**, for prescribed organisations
4. **Expanded scope**, applying to data controllers and now data processors
5. **Expanded definition** of personal data, including online identifiers
6. **Expanded reach**, applying to organisations within or targeting the EU
7. **New rights for data subjects**, including the right to be forgotten and the right to data portability
8. **Easier access by individuals to their own data**, including a right to more extensive information

A roadmap to GDPR

Nick Gibbons, a Partner at BLM and specialist in data protection law, advises that the ICO has made clear that she regards accountability as a critical part of GDPR compliance. In the ICO's own words:

"...arguably the biggest change is around accountability. The new legislation creates an onus on companies to understand the risks that they create for others, and to mitigate those risks. It's about moving away from seeing the law as a box ticking exercise, and instead to work on a framework that can be used to build a culture of privacy that pervades an entire organisation."

1 Forming the team

- Form a 'GDPR committee' of stakeholders across a range of functions:
  Information security and technology, heads of businesses, governance and compliance, HR, customer services and marketing
- Identify an 'ally' at Executive management or Board level with an understanding of GDPR, to assisting in decision-making and securing resources

"The compliance and governance team were vital for understanding the legal intricacies of the regulations. Additionally, their knowledge of the nature and infrastructure of the business supported me in assessing how the legal changes become practical business actions."

Data protection officer

2 Initial review

- Initial gap analysis of existing and new regulations
- Understand the current GDPR compliance position of the business through questionnaires and workshops with business units and identified stakeholders
- Identify where new processes must be developed and where existing processes must be enhanced

"We are documenting the review process and all remedial actions taken and why, e.g. how we selected a data retention policy. The GDPR doesn't provide explicit rules, so early compliance audits could simply look for evidence that the regulations have been reviewed and considered in the context of organisations."

Scott Wilson, chief information security officer, Ventiv Technology

3 The data protection officer (DPO)

- Identify an individual who understands the business processes and infrastructure, and can communicate with legal, IT and the business.
- Ensure the DPO position is neutral, i.e. doesn't sit within HR or in-house legal or involves data processing activities
- Review the DPO job description, powers and authority to evidence the DPOs independence

"The DPO must retain independence whilst understanding the business. We have therefore chosen to split the role into two: an 'operational' DP Manager who understand the business's data processing, and a more independent, 'reporting' DPO with compliance knowledge who can interact with the regulator but isn't directly involved in managing day-to-day data processing activities."

Data protection and privacy officer

4 Data map / information asset register

- Develop an asset register for each business unit identifying:
  What personal data is held
  What category it falls into (HR, customer etc)
  Where it is held (both in online systems and physically)
  Where it is transferred to and from (including third parties and across borders)
  How the data is used/processed
  Any specific security arrangements in place
  The legal basis for using the data
- Develop a data retention policy for each data type

"Creating a data and data processing map was the essential start in understanding how GDPR relates to the organisation. But the process is lengthy and not without challenge! I worked with an identified and trained 'GDPR business support manager' for each unit. Using data categories already well established across the organisation and software that avoids 'double keying' helped keep momentum."

Mike Davies, data protection officer

5 Understand roles and those of third party vendors

- Document data processing where you act as a data processor or controller
- Incorporate data management language into contracts with third-party processors/controllers
- Consider requiring vendors to meet specific codes of conduct or hold appropriate certification, e.g. ISO 27001
- Understand how past third-party data processors have acquired, stored and deleted data

"Due to the scale and scope of our organisation, we prioritised mapping any overlaps of our data controlling and processing activity. We examined the associated reporting lines between our business units, third-party vendors and data subjects."

Group data protection officer

6 Privacy impact assessments and risk improvements

- Consult IT, system security and data owners to understand the risks of harm to individuals through the misuse of data processing activities
- Prioritise high-risk activities, including individual profiling, large-scale personal data processing and large-scale monitoring of public places
- Undertake the risk assessment for no controls, existing controls and proposed controls to develop a risk improvement programme

"As GDPR increases the focus on risk management, we have mapped the impact of GDPR non-compliance against each of our organisation's principal risks. This helped prioritise risk improvements, which we further refined by looking at the scale of each improvement task and the dependencies between them."

Data protection officer

7 Breach notification procedures

- Update data protection policies to meet GDPR requirements, i.e. the data protection manual
- Understand the existing breach identification, response and reporting process
- Develop a testing and audit programme for breach response protocols
- Require view of vendor breach responses and testing programme
- Prepare a disclosable data breach log

"To meet the 72-hour reporting deadline we have developed a 24/7 proactive breach monitoring and response process and communicated this to all employees. Our technical response has been enhanced by incorporating the actions that deal with operational, legal and PR aspects of the breach."

Data protection and privacy officer

8 Capturing consent

- Review and update all privacy notices to align with GDPR, including information provided directly to customers and employees, and on public websites
- Review how data subjects are currently informed of your processing of their personal information
- Consider the shift from opt-out to opt-in consent and how previous opt-out subjects can be legally contacted after implementation

"Address privacy and cookie statements on websites, apps and paper forms immediately. This will be an easy test for regulators to spot non-compliance on day one."

Scott Wilson, chief information security officer, Ventiv Technology

9 Data subject access requests

- Develop practical processes to verify, review and respond to data subject access / erasure requests
- Consider the differences between internal and external subject requests
- Understand where the organisation has a legal ground to decline access or erasure requests
- Develop a data deletion policy that evidences how and when data is deleted

"We have independently verified all actions we have taken, including using an external law firm to assess the regulations and an external auditor to review the process changes we have made."

Mike Davies, Data protection officer

10 Education and training

- Introduce several training and education methods, including:
  data protection training at new employee induction
  Online compliance tests for all staff
  One-on-one training for identified individuals across each business unit, data committee, etc.
  Breach response 'drills'
- Maintain an awareness programme, including:
  Online countdown to GDPR on employee intranet
  Town hall meetings and Q&A sessions

"We have shifted the focus from scarily large fines and strict reporting requirements to a need for openness and sharing across the business. A 'no blame' culture will be required to encourage employees to report breaches and incidents immediately."

Data protection and privacy officer

11 Ongoing review

- Request for review of any proposed data processing before any new data collection.
- Educate on the principle of 'privacy by design', i.e. where data protection can be addressed in the planning stage of new processing
- Develop a testing and auditing calendar for data collection, processing and deletion. Agree similar processes that be followed by third-party processors
- Be aware of how regulations are interpreted by data subjects and regulators after implementation

"We have established the infrastructure and are now focusing on checking that the right data is making its way into this infrastructure and testing processes. Following implementation, we will monitor the regulatory environment refining our processes to match the claims, requests and breaches that emerge."

Group data protection officer

GDPR: IMPLICATIONS FOR INSURANCE MANAGERS

Storage Don't rely on multiple spreadsheets, which make processing, duplication and transfer almost impossible to monitor. A central, unified system that links to the overall business will aid compliance.

Transfer Work with the DPO to document the 'data chain' from the organisation to insurers, via brokers etc. Agree contractual clauses and the process of auditing the data storage and processing with each link of the chain.

Insurance cover The cost of GDPR breaches may to a large extent be picked up by a combination of cyber, professional indemnity and D&O insurance, but this will depend upon individual policy wordings and it would be prudent to discuss the extent of your existing cover with your brokers now. Although cyber insurance explicitly covers the loss or theft of personal data and provides indemnity and support for breach investigation and notification it may not cover other breaches of GDPR. Moreover, although GDPR doesn't state that fines for non-compliance are uninsurable, the position is uncertain because there is as yet no specific caselaw on the issue. Insurers who do insure unintentional breaches GDPR are clearly likely to require organisations to demonstrate at least a reasonable degree of compliance with GDPR as a precondition of cover.

Deletion Carefully document the retention policy for claims information. Take a practical approach whilst acknowledging any legal storage requirements. Document why longer retention periods have been adopted for some types of information.

airmic

WHITE PAPER

6 LLOYD'S AVENUE,
LONDON,
EC3N 3AX

TEL: +44 207 680 3088
FAX: +44 207 702 3752
EMAIL: ENQUIRIES@AIRMIC.COM
WEB: WWW.AIRMIC.COM