GDPR – 2020

INTRODUCTION

EU **member states have now operated within the General Data Protection Regulations (GDPR) for 18 months since they came into force on 25 May 2018, bringing with them a huge change in data protection law.**

The GDPR seeks to balance the privacy rights of individuals with the capacity of businesses to use data for their own purposes in the internet era. In most organisations, the IT and Data Privacy teams have led the compliance project. However, risk managers have had a major role to play in ensuring that the risk of non-compliance is understood by all employees and stakeholders (e.g. contractors and suppliers) and that the organisation develops a GDPR-aware culture. Complying with the GDPR is an enterprise risk that requires organisation-wide change. As major breaches of the regulations and the implications of these are announced, Airmic members can continue to support their organisations in navigating the changing road map to compliance.

This white paper, developed with BLM, follows two previous Airmic papers on the GDPR (see details below) and highlights some of the notable developments since the law came into force and the implications for organisations.

- The EU General Data Protection Regulations: What risk managers need to know (Airmic 2017).
- GDPR Goes Live: A framework for Airmic members (Airmic 2018).

A REMINDER: MAJOR PROVISIONS

1. Mandatory reporting of data breaches within 72 hours.
2. Hefty fines of up to the greater of 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.

GDPR: THE PRACTICAL CONSEQUENCES SINCE MAY 2018

Despite the noise surrounding the GDPR coming into force, the consensus was that there would be significant delays before breach investigations by the Information Commissioners Office (ICO) would lead to hefty fines. Organisations anticipated a lenient approach from regulators and hoped that by taking action to investigate the data they hold and how it is processed, they would be considered compliant. However, the extremely high-profile investigations into organisations such as British Airways, coupled with a heightened public consciousness of data protection issues and the rights of individuals, means that the GDPR is something organisations must continue to consider and address. Airmic member organisations have experienced the following changes:

- A vast increase in the number of data breach notifications they are making to the ICO.
- A challenge in meeting the 72-hour reporting requirement.
- IT and Data Privacy teams being the focus during investigations.
- Major increases in investigation costs and liability payments.
- A tolerance from the ICO towards small businesses but some headline fines imposed on major corporates.
- A tendency of the public to exercise the new subject access rights more than any other GDPR rights.
- A much greater consciousness of the accountability principle.

The ICO is under a huge strain, with some reports stating that its notification hotline is receiving 500 calls a week, at least a third of which are quickly identified as concerning issues that do not need to be reported. This highlights the incredibly cautious approach being taken by organisations in the UK.

Tim Smith says: "There is increased awareness (often through training received at work) on the part of individuals as to their rights under the GDPR and the Data Protection Act 2018, and the obligations imposed on organisations. This, coupled with awareness of breaches, some favourable decisions from the courts and claims farming by claimant lawyers, has led to an increase in the number of such claims."

A CHECKLIST FOR RISK MANAGERS: 7 QUESTIONS TO ASK NOW AND 7 CON

Complying with the GDPR is not a one-off project. An integrated, thorough and transformationa
systems handle personal data. Compliance programmes must be ongoing and iterative, consider

QUESTIONS TO ASK NOW
Is our GDPR implementation plan being assessed in line with the compliance landscape, including the consequences of a no-deal Brexit?
Have all implementation actions been rigorously followed through?
Has the initial GDPR compliance risk assessment been refreshed?
Are the controls still relevant and the risk owners reporting as agreed?
How regularly is GDPR non-compliance risk information being communicated across the business and supplier ecosystem?
Are GDPR breach crisis management plans in place and how regularly are they tested?
Are the C-suite and Board being kept advised on GDPR compliance, near misses and actual events?

ITINUOUS STEPS TO TAKE

al programme is required that addresses how an organisation's personnel, processes and
ring lessons learned and best practice, and testing procedures.

ACTIONS TO REGULARLY TAKE

Examine the ICO's updated guidance. Recent updates cover subject access requests, unfounded and excessive requests, and special category data.

Consider appointing a GDPR representative within the EU to assess data flows and transfers into other EU states. The GDPR representative can also review processing agreements to ensure the UK's Data Protection Act is covered and the UK is referred to as separate to the EU.

Ensure that data processing mapping is an ongoing exercise as this underpins all compliance. Highlight where new technologies may be introducing new data processing.

Update the privacy notice to capture new data processing and bring information on collection, processing and retention periods together into a clear and transparent document.

Implement and routinely review a DPIA (Data Protection Impact Assessment) process, recording outcomes.

Review the role of the Data Protection Officer to understand if they have the freedom and access to carry out the role, and identify if any conflicts of interest have appeared within their day-to-day role.

Shift focus to accountability by supporting risk owners in recording the actions they have to take to understand the risks to individuals in the way they process data and how those risks should be mitigated.

Establish specific processes for responding to subject access requests from existing and previous employees. There has been a surge in these and this is an area of interest for the regulator.

Develop processes to test and report on the GDPR awareness of all employees, including phishing training.

Update practical training beyond GDPR awareness to address processes or teams where issues have arisen.

Amend response and reporting plans to demonstrate that the organisation has learned from personal data breaches or near misses.

Speak to insurers about their incident investigation processes as these have been identified as a potential source of best practice.

Challenge the Board-level individual with data protection responsibility on the actions they have taken to address GDPR incidents and how they are instilling a data protection-aware culture, highlighting their accountability.

Investigate GDPR compliance within the supplier ecosystem from a governance perspective as well as at the IT level.

WHAT CAN AIRMIC MEMBERS LEARN FROM THE MAJOR INVESTIGATIONS AND FINES SO FAR?

In July last year, the ICO announced its intention to fine British Airways £183.4 million and Marriott £99.2 million. These were "notices of intent" rather than final determinations and the ICO has recently announced that the period for challenging the notices of intent has been extended until 31 March 2020.

Key takeaways:

- Businesses can reduce fines by co-operating with investigations and taking steps to swiftly identify the cause of the incident, rectify the data, notify affected individuals and implement security improvements.
- Organisations must develop robust processes for checking the data protection protocols and controls of third parties. The distraction of a merger or acquisition can drag away resource at a time when the GDPR risk is at its highest.
- The ICO is not just focusing its investigations on technology firms, as some expected.
- As well as fines, regulators are also using their right to issue 'stop processing' notices, which require an organisation in breach of the GDPR to cease the particular data processing that is being investigated.
- The complex issues of "consent and transparency" underpin many complaints. Organisations must demonstrate that they are clear and concise when describing to data subjects how they use their personal data.
- The ICO is adopting a tough stance even where the breach is the work of an external party or a criminal hack. Organisations must demonstrate that they are taking data privacy seriously.

How can cyber insurance support organisations?
The availability and benefits of cyber insurance have become clearer as organisations have improved awareness of their obligations, have been hit with data access requests and breaches, and have stress tested gaps in existing cover. Investigation costs and liability payments have risen as breaches and incidences of cyber-crime have risen. As claims start to hit, cyber products are becoming more refined and tailored. Airmic members have had success in using this awareness to begin meaningful conversations with their IT and Data Privacy teams around cover.

The GDPR is a sweeping set of rules which has created a wider range of triggers and broader potential breaches than those catered for within a typical cyber policy. BLM highlights that insurer-backed incident response teams are swift and effective in unravelling breach incidents, which supports organisations meeting the 72-hour reporting requirements, and in demonstrating to the ICO that action has been taken to contain a breach and prevent it happening again. In most cases, investigation costs, restoration costs, and other costs and liabilities associated with the breach are insurable. However, the ultimate question for organisations is whether GDPR fines and penalties can be covered, as these have the potential to be huge in size and their insurability varies by local law.

Organisations should seek affirmative cover for fines and penalties for a breach of the GDPR, where insurability is possible.

Key factors in answering the insurability question will likely include:

- What is the nature of the fine or penalty and what has led to the non-compliance?
  Intentional or reckless wrongdoing?
  Strict or no-fault liability?
  Negligence?
- Does the policy expressly provide or preclude coverage?
- What is the choice of law provision in the policy?
- What are the decisions of the courts in the relevant jurisdictions?

"IN ORDER TO MAXIMISE THE POTENTIAL FOR RECOVERY, YOU SHOULD CHALLENGE STANDARD POLICY EXCLUSIONS THAT PRECLUDE INSURANCE COVERAGE FOR FINES UNLESS THEY ARE 'INSURABLE UNDER THE APPLICABLE LAW'. TO DO SO, YOU SHOULD SEEK GREATER CERTAINTY BY PREVENTING INSURERS FROM DENYING CLAIMS UNLESS THEY ARE EXPRESSLY PROHIBITED BY A COURT WITHIN THE APPROPRIATE JURISDICTION. DOING THIS REMOVES THE POTENTIAL FOR INTERPRETATION OF COMMON LAW BY INSURERS' CLAIMS TEAMS AND PUTS THE ONUS ON AN INDEPENDENT THIRD PARTY TO PREVENT RECOVERY."

GRAEME NEWMAN, CHIEF INNOVATION OFFICER, CFC UNDERWRITING

POSTSCRIPT: GDPR & COVID-19

With the outbreak of COVID-19, a number of implications for the GDPR have arisen which bear some attention:

- The ICO has indicated that they will not penalise organisations which need to prioritise matters other than data protection during this period.
- The ICO cannot extend the statutory deadlines but will tell individuals that they may experience understandable delays.
- Organisations need to consider the same security measures for homeworking as they would use in normal circumstances.
- Staff can be told about COVID-19 cases in the organisation, but would probably not need to be told the names of those concerned.
- It is reasonable to ask people if they are experiencing COVID-19 symptoms.
- The ICO has seen an increase in criminals using the situation to set up scams using nuisance calls, emails and texts.

In addition, in a note issued on 15 April 2020, the ICO has said:

- They recognise that the current reduction in organisations' resources could impact their ability to comply with aspects of the law.
- When handling complaints about organisations, the ICO will take into account the impact of the crisis. The ICO will give organisations longer than usual to respond to or rectify any breaches associated with delay if the organisation is recovering its service and gradually improving timescales.
- Organisations should continue to report personal data breaches within 72 hours of becoming aware of the breach. However, the ICO acknowledges that the current crisis may impact on this.
- When conducting investigations, the ICO will act knowing that there is a public health emergency and will seek to understand the challenges faced by organisations. This may mean that the ICO uses the power to require organisations to provide them with evidence less often and will allow more time to respond.
- In deciding whether to take formal regulatory action (including the imposition of fines), the ICO will take into account whether the organisation's difficulties result from the crisis and if the organisation has plans to put things right at the end of the crisis. The ICO may also give organisations longer than usual to rectify any breaches that predate the crisis where the crisis impacts on their ability to take steps to put things right.
- All formal regulatory action in connection with outstanding information request backlogs will be suspended.
- Before issuing fines, the ICO will take into account the economic impact and affordability. In the current circumstances, that is likely to mean that the level of fines is reduced.
- The ICO may not enforce against organisations who fail to pay or renew their data protection fee if the organisations can show that this is specifically due to economic reasons linked to the present situation, and provided the ICO is adequately assured as to the timescale within which payment will be made.
- The ICO will recognise that the reduction in organisations' resources could impact on their ability to respond to Subject Access Requests where they need to prioritise other work due to the current crisis.

In addition, the National Cyber Security Centre has said that:

- They have detected a rise in UK government branded scams.
- Overall levels of cybercrime have not increased.
- The surge in homeworking has increased the use of potentially vulnerable services (such as some Virtual Private Networks that are known to have vulnerabilities).
- Threats include phishing emails with "coronavirus" or "COVID-19" in the subject line (examples include "2020 Coronavirus Updates, 2019-nCov: New confirmed cases in your City") or purporting to be from the World Health Organization or a medical professional, malware with similar terms in links, the registration of domain names with these terms in them and attacks against newly (and often rapidly) deployed remote access or remote working infrastructure.
- They have also identified a malicious Android App purporting to be a coronavirus outbreak tracker and text scams suggesting that payments are going to be made to individuals by the government.
- In this respect, it is anticipated that further scams will be linked to any government compensation schemes.
- Health organisations are coming under particular attack as they are obviously under strain.
- Malicious actors are also seeking to exploit the increased use of popular communications platforms (e.g. Zoom) to send phishing emails with links to malicious files that have words such as "Zoom" in the links.
- They have issued a number of guidance documents and material on mitigating the risks – for individuals, organisations and cyber security professionals.