The impacts of the GDPR on Corporate Governance practices in the GCC

The European Parliament and Council passed a regulation (EU) 2016/679 to refresh the data and privacy protection laws for European Union States. The new regulation is commonly known as the General Data Protection Regulation (GDPR) and came into effect on 25 May 2018. The GDPR has defined the rights of EU individuals relating to how their data is collected, stored, processed and used by organisations. Any organisation that handles the data of any EU citizen is bound by the provisions of the GDPR. This regulation is applicable globally and fines of up to 4% of worldwide turnover or 20 million euros (whichever is greater) will be levied on businesses breaching them. GCC organisations and businesses need to consider whether they collect, store, process or control any data for EU citizens and revise their own governance and enterprise risk management frameworks to comply with the GDPR provisions.

A robust Corporate Governance framework as the foundation for business excellence and compliance with the General Data Protection Regulation (GDPR)

Due to increased concerns of breaches of privacy and misuse of personal data for individuals, the European Union repealed Directive 95/46/EC (the old data protection directive) and replaced it with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (GDPR or the Regulation). The Regulation has an international reach and covers any organisation worldwide that collects, controls, processes or uses the information (data) of any EU citizen. The Regulation is available in multiple languages here:

The UK's largest data protection agency the Information Commissioner's Office (ICO) has aligned the updated UK data protection regulation 2018 with the GDPR and they have also issued extensive guidance to assist organisations become compliant.

The below are some useful tools and guides provided by the ICO to prepare and explain what is required to be GDPR compliant and remain within the provisions.

Data Protection Self-Assessment

Getting ready for the GDPR

Case studies

Many organisations do not fully understand the impact of the GDPR and how it will affect their business operations going forward. Some key points covered by the Regulation:

- Fines of 4% of revenue or 20 Million Euros (serious operational failures),
- 72 hours to disclose any material data breaches,
- Covers all European Union citizens worldwide,
- Some organisations now require a Data Protection Officer,
- Board of Directors have a fiduciary duty to set the IT strategy – covering security, data and controls,
- Greater need to understand what data organisation holds, where it is stored, processed and controlled,

- Individuals have the right to access their data, request corrections and even be forgotten,
- Fines of 2% of revenue or 10 Million Euros (minor/technical breaches).

GDPR–the beginning of the data protection and privacy journey for many GCC businesses

GCC businesses should review whether they hold data or information of any EU citizen and also consider whether the data is sufficiently minimised as per the Regulation requirements. If GCC organisations hold data of EU citizens and have not already implemented procedures on how they collect, store, process and control that data then they should urgently look at their IT policies, internal control procedures and enterprise risk management framework. A general review and update of their overall governance framework is likely to be required to integrate and simplify who is accountable for making decisions and how breaches may be reported internally and escalated.

Organisations can follow the below roll-out plan to review and prepare to comply with the Regulation:

- Preparation and educate staff,
- Roll-out and provide guidance,
- Regularly audit and perform a gap analysis,
- Improve controls, processes and procedures and
- Repeat the cycle all over again.

All businesses that store and process data of EU citizens should review their processes, IT systems, internal controls, hardware, software and applications to be GDPR compliant and to conduct data risk impact assessments for new projects where personal data is collected, stored, processed and controlled.

Article 5 of the GDPR sets out seven key principles which lie at the heart of the general data protection regime:

Article 5(1) requires that personal data shall be:

"(a) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."

The ICO provides a 12-point guide and checklist for organisations to consider when preparing to comply with the GDPR:

1. Ensure senior/key people are aware of the GDPR and appreciate its impact.

2. Document any personal data you hold, where it came from and who you share it with. Conduct an information audit if needed.

3. Review your privacy notices and plan for necessary changes now that the GDPR has come into force.

4. Check your procedures cover all individuals' rights under the legislation–for example, how you would delete personal data or provide data electronically in a commonly used format.

5. Plan how you will handle subject access requests within the new timescales and provide any additional information.

6. Identify and document your legal basis for the various types of personal data processing you do.

7. Review how you seek, obtain and record consent. Do you need to make any changes?

8. Put systems in place to verify individuals' ages and, if users are children (likely to be defined in the UK as those under 13), gather parental consent for data processing activity.

9. Make sure you have the right procedures in place to detect, report and investigate a personal data breach.

10. Adopt a "privacy by design" and "data minimisation" approach, as part of which you'll need to understand how and when to implement Privacy Impact Assessments.

11. Designate a Data Protection Officer or someone responsible for data protection compliance; assess where this role will sit within in your organisation's structure/governance arrangements.

12. If you operate internationally, determine which data protection supervisory authority you come under.

Click here for the full paper from the ICO:

Organisations handle risk management in different ways. The GDPR offers guidance on the risks that organisations should formally identify, namely: emerging privacy risks, this should include new projects. A register should be maintained of the processing activities and internal inventories created. Any organisation planning on conducting any high-risk data processing activities must complete a data protection impact assessment. Under a certain criterion it will be compulsory to appoint a Data Protection Officer.

The protection of natural persons should apply to the processing of personal data by automated means, as well as to manual processing. The Regulation includes the following rights for individuals:

1. the right to be informed,

2. the right of access,

3. the right to rectification,

4. the right to erasure,

5. the right to restrict processing,

6. the right to data portability,

7. the right to object, and

8. the right not to be subject to automated decision-making including profiling.

Governance framework and GDPR

A robust Corporate Governance framework can effectively manage risk, including the requirements of the GDPR and other laws and regulations.

Corporate Governance definitions

"Corporate governance involves a set of relationships between a company's management, its board, its shareholders and other stakeholders. Corporate governance also provides the structure through which the objectives of the company are set, and the means of attaining those objectives and monitoring performance are determined." **The OECD Principles of Corporate Governance**

"Corporate Governance refers to the way in which companies are governed and to what purpose. It identifies who has power and accountability, and who makes decisions. It is, in essence, a toolkit that enables management and the board to deal more effectively with the challenges of running a company. Corporate governance ensures that businesses have appropriate decision-making processes and controls in place so that the interests of all stakeholders (shareholders, employees, suppliers, customers and the community) are balanced."- **ICSA, The Governance Institute**

Governance overview for GCC organisations and GDPR considerations to mitigate risks to the directors for breach of their fiduciary duties

The board of directors of an organisation is tasked with the control, oversight and setting the risk appetite and tolerance for the company in-line with the mission, vision, values and the strategic plan for the business. One major concern for directors internationally and in the GCC is the increasing risk of cybercrime, IT security and unauthorised access to data and information. With the GDPR we are seeing an amplified focus on developing the safeguards around IT systems, security, encryption, backups and control of data and information.

The GDPR has a global reach and any organisation which controls, processes or uses the data and information of EU citizens is required to protect the privacy and freedoms of these individuals. Organisations need to demonstrate they have the requisite enterprise risk management solution in place to identify the current and emerging risks concerning the privacy and freedoms of individuals and have effective procedures to mitigate risks, inform and report data breaches to the supervisory body, the ICO or other relevant organisation regarding any material breach or break down of operational controls, and continually monitor and improve controls. Risks should be treated appropriately, either eliminated, mitigated, transferred or accepted.

Boards are ultimately responsible for implementing a robust corporate governance framework, which should include an enterprise risk management framework. Usually the audit or risk committee consider the risks which will now include the requirements under the GDPR. In order to establish sufficient procedures, systems and controls an IT steering committee can do a lot of the legwork for the audit or risk committee to identify, monitor and improve any gaps in the risk management for data and information storage, processing and control. The GDPR provides guidance on how organisations can implement risk impact assessments for projects which involve personal data and information of individuals, especially for EU citizens.

The GDPR reaffirms that individuals have the right to privacy and freedom. The regulation provides mandates on how organisations should safeguard and use personal data, what data should be stored (only relevant information and what is necessary), how data is processed and ultimately controlled. Data security should be by design and by default. The aim of the GDPR is to ensure that the personal data of

individuals is secured globally for EU citizens. Data protection and security is about processes, IT infrastructure and the people who have authorised access to use or transfer that data. The GDPR highlights three main elements for the security and protection of data. Organisations must evaluate the data they hold, they need to safeguard and secure that data and monitor to detect any gaps or breaches. End to end encryption is seen as a necessary safeguard to ensure that data even if obtained unlawfully will not be accessible or usable by the perpetrator. Other safeguards can be used such as smart cards, two level authentication, token encryption and controlled user access to operating systems, software and applications. Organisations can limit their IT risk by minimising the number of access points or vectors and by using virtual machines and hypervisors–the process that separates a computer's operating system and applications from the underlying physical hardware to minimise vulnerabilities.

Technology, IT security, IT systems and the future

The speed of technological advances has caught many organisations unawares. If we think about some of the recent major issues with data breaches, data crypto viruses and hacking, too many businesses have failed to develop their IT infrastructure, systems and software at the same pace as vulnerabilities were being exploited. From a governance point of view, an organisation should consider scenarios and plan to mitigate and have contingencies and business continuity plans in place. They should also consider disaster recovery and complete systems failures; all plans and mitigations should be tested to see if they work in practice.

Organisations may consider implementing or integrating the following standards to minimise data privacy risks ISO 27000, ISO 27001 and BS-10012 "Information Governance". As part of these standards, organisations should endeavour to gain certification and continually improve their systems, applications and policies. As businesses move towards artificial intelligence (AI), automation and the use of blockchain technologies, it is even more important to adopt internationally recognised standards for IT security, information governance, privacy and confidentiality. With the use of AI and automation, organisations need to consider the impacts of the GDPR on the personal rights of privacy and freedoms of EU citizens. The Regulation speaks to the use of AI and how organisations need to balance the benefits of AI and automation with the rights and freedoms for EU citizens and other customers.

Most international organisations are still coming to grips with the GDPR requirements and how they will impact them. It is likely that the Regulation will become the international standard on data privacy and protection for individuals. There is a pressing need for GCC organisations and businesses that handle the data for EU citizens to embrace the principles of the GDPR and implement policies and procedures to safeguard all the data and information they store, process, control and transfer as the reputational risk for loss or breach of data is high.

Robert L. Ford
Managing Partner, Governance Gurus FZE
rob@governance-gurus.ae
+971 04 387 3554
+971 055 8034 055
www.governance-gurus.ae
Robert is the Managing Partner of a governance consulting enterprise called Governance Gurus FZE. The company provides strategic consulting and CPD accredited workshops and training to businesses across the region and internationally. He is a regional thought leader and subject matter expert and is regularly asked to speak on corporate governance, compliance, enterprise risk management and change management matters and provides his clients with training and workshops too.

Robert advises the Senior Management teams and Boards of numerous organisation across the Middle East, Asia and Europe. He is an investor and on the Board of two UAE businesses. He is also the Vice-Chairman of a Gulf Forum which brings together some of the leading thought leaders on corporate

governance, risk management, compliance and company secretarial best practice. Robert provided corporate governance advisory services to the Board and Committees of the Dubai Properties Group (DPG), a member of Dubai Holding. He worked closely with the Chairman and the Group CEO to enhance the Corporate Governance Framework across DPG and its verticals and helped develop their Risk Appetite Compliance Assessment.

Robert holds a master's degree in Leading Innovation & Change from York St John University and is also a qualified Governance Professional and Chartered Secretary (FCIS) and member of the UK Institute of Directors (for over 10 years) and a member of STEP–the Society of Trusts and Estate Practitioners. Robert is also part way through a Master's Degree in HRM & Training with the University of Leicester.