MGC & KNAV
GLOBAL RISK ADVISORY LLP
PARTNERS BEYOND BOUNDARIES

General Data Protection Regulation ('GDPR'); Information privacy and security

The European Parliament adopted the GDPR in April 2016, requiring certain classes of companies in accordance with the criteria for applicability to protect personal data and privacy of the citizens of the European Union ('EU') for transactions that occur within the 28 EU member states.

What does this change mean for these EU companies? How does this impact the scope and purview of personal data and privacy? What must these companies do to ensure compliance and adopt this change?

This thought leadership paper,that contains the views of our Associate Partner, Tarun Kher, explains the above.

Applicability

GDPR compliance is applicable to all companies that process and archive personal information *(including personally identifiable data within social media, photos, email addresses and IP addresses)* relating to EU citizens within EU states, even if such companies do not have a business presence within the EU. The ensuing categories of companies are required to adhere with the provisions of GDPR:

- Those that have a presence in an EU country;
- Those that have no presence in the EU, however the Company processes personal data of European residents;
- Those with over 250 employees; &
- Those with fewer than 250 employees but where the Company's data-processing impacts the rights of individuals *(data subjects)*, is not occasional, or includes certain types of sensitive personal data.

Compliance responsibility | Data protection officers

GDPR defines specific roles and responsibilities for ensuring compliance viz. data controller, data processor and the data protection officer ('DPO') respectively.

The data controller defines the methodology for processing personal data and defines the objectives for which data is processed. Data processors are generally represented by internal groups or external outsourcing firms that maintain and process personal data records and are held liable for breaches or non-compliance.

Data controllers and data processors are mandated to appoint a DPO in cases where Companies process or archive significant volume of data relating to EU citizens , process or archive privileged personal data, regularly monitor pertinent data subjects, or are a public entity *(except law enforcement authorities, which may be exempt)*.

The primary objective behind the appointment of the DPO is to designate someone with the responsibility of overseeing the data security strategy.

Overview of key components

i) Data privacy by design ('DPD')

Processes will need to be continuously assessed and periodically amended to consider privacy by design wherein the data controller must apply adequate technical and organisational procedures to comply with the requirements of GDPR and protect the rights of data subjects.

The types of privacy data protected by GDPR includes:

- Basic identity information such as name, address and ID numbers;
- Web data such as location, IP address, cookie data and RFID tags;
- Health and genetic data;
- Biometric data;
- Racial or ethnic data;
- Political opinions; &
- Sexual orientation.

ii) Data portability

Personally identifiable data must be portable by open use of common file formats that are machine-readable when the data subject receives them.

iii) Rights of data subjects

The data controller is obligated to provide a free electronic copy of any personally identifiable data to the data subject. GDPR provides the following rights to data subjects from the respective data controllers:

a) Right to access: To confirm whether their personally identifiable data is being processed along with the objective for which it is being processed and the location;

Head office: Suite 219 to 221 Square One Building, Saket District, New Delhi 110 017
Other offices: Amsterdam | Atlanta | Bengaluru | Geneva | Hyderabad | Kolkata | London | Lyon | Mumbai | Singapore | Toronto

b) Right to be forgotten: includes permanent or on-demand deletion of his/her personally identifiable data, cease further distribution of the data, and demand third parties' restriction on processing of the data.

iv) Data breach notification

As a data breach is likely to result in a risk to the rights of individuals, GDPR requires a mandatory breach notification to be submitted to the supervisory authority within 72 hours of the organisation first becoming aware of the breach. In addition, data processors are required to notify their customers without unnecessary delay.

v) Consent

GDPR requires "a statement or clear affirmative action" that signals agreement of transferring personal data. Further parental consent is required for processing children's *(13-16 years of age depending on member state)* personal data.

Penal consequences

The GDPR allows for steep penalties of up to €20 million or 4 percent of global annual turnover, whichever is higher, for non-compliance. Failure to adequately conduct a Data Protection Impact Assessment ('DPIA') where appropriate is a breach of the GDPR and could lead to fines of up to 2% of an organisation's annual global turnover or €10 million – whichever is greater.

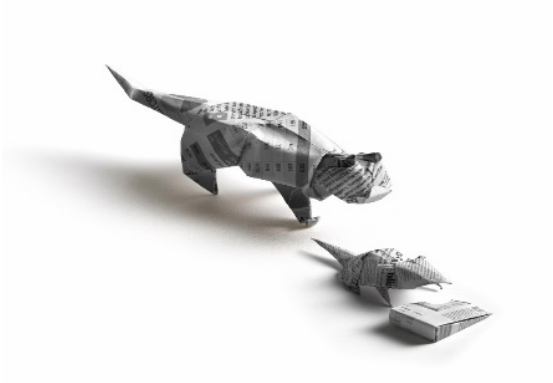
Mapping IT security, governance and GDPR

Compliance with GDPR will require an IT governance framework to be modified to incorporate pertinent aspects relating to data transfer, data subject consent, and privacy by design. GDPR introduces several privacy arrangements and control mechanisms that are intended to safeguard personally identifiable information. Most of these controls are also recommended by ISO/IEC 27001:2013, ISO/IEC 27002:2013 and other "ISO27k" standards, as well as COBIT 5.

For example, ISO27K controls, such as A.18.1.4 and A.9.1.1, relate to privacy and risk assessment and can be interpreted as addressing privacy concerns around data transfer or privacy by design in relation to personally identifiable information or data subject information. COBIT 5 also refers to privacy officers with responsibility for screening the risk and organisational impacts of privacy regulations while ensuring such legislations are complied with. This definition is similar to article 37 of GDPR with its requirement for the designation of a Data Protection Officer ('DPO').

To work towards ensuring compliance of their data, organisations should take the following actions guided by seven key GDPR principles:

- **Lawful, fair and transparent processing:** This principle emphasizes on transparency for all EU data subjects;
- **Purpose limitation:** This principle means that organizations need to have a lawful and legitimate purpose for processing the information in the first place.
- **Data minimization:** This principle instructs organizations to ensure the data they capture is adequate, relevant and limited.
- **Accurate and up-to-date processing:** This principle requires data controllers to make sure information remains accurate, valid and fit for purpose.
- **Limitation of storage in the form that permits identification:** This principle discourages unnecessary data redundancy and replication. It limits how the data is stored and moved
- **Confidential and secure:** This principle protects the integrity and privacy of data by making sure it is secure (which extends to IT systems, paper records and physical security).
- **Accountability and liability:** This principle ensures that organizations can demonstrate compliance.



MGC & KNAV Global Risk Advisory LLP
Head office: Suite 219 to 221 Square One Building, Saket District, New Delhi 110 017
Other offices: Amsterdam | Atlanta | Bengaluru | Geneva | Hyderabad | Kolkata | London | Lyon | Mumbai | Singapore | Toronto

Conclusion | Data protection impact assessments

DPIAs help organisations identify, assess and mitigate or minimise privacy risks with data processing activities. Such assessments are particularly relevant when a new data processing system or technology is being introduced.

DPIAs also support the accountability principle, as they help organisations comply with the requirements of GDPR and demonstrate that appropriate measures have been taken to ensure compliance.

A DPIA should be conducted as early as possible within any new project lifecycle, so that its findings and recommendations can be incorporated into the design of the processing operation.

The GDPR comes into force on May 25, 2018. With a comprehensive plan in place well in advance, organisations that act as data controllers or processors will be able to ensure compliance with the new rules in a timely manner, including implementing an adequate testing period.

Organisations will need to conduct DPIA and investigate their current/'as is' IT security and data assurance practices to perform a gap analysis and identify the 'to be' practices for timely implementation.

About us:

MGC & KNAV Global Risk Advisory LLP ('MGC & KNAV'), is a member firm of KNAV International Limited, ('KNAV'). MGC & KNAV has recently been rated amongst the top 10 GRC consultants in India and has also been recognised as 'the company of the month' in January of 2018 by CEO Magazine.

MGC & KNAV serves organizations in Canada, France, India, Netherlands, Singapore, Switzerland, United Kingdom & USA; who are seeking seamless and value driven services in the areas of risk management, control assessments, internal audits, process reengineering, governance frameworks, human resources, CxO transformation and for their research requirements.

KNAV is a registered trademark of the United States patent and trademark office. KNAV International is a US not-for Profit Corporation. KNAV refers to one or more of the member firms of KNAV International, each of which is a legally separate and independent entity. The member firms of KNAV are leading firms, providing audit, tax and advisory services across the globe.

For expert assistance, please contact:

- Monish Gaurav Chatrath | monish.chatrath@knavcpa.com | +91 98113 03000 or +1 404 820 2101
- Tarun Kher | tarun.kher@knavcpa.com | +91 9810421632

Visit us at: www.knavcpa.com | www.mgcknav.com