DATA PROTECTION A THREAT

General Data Protection Regulation introduced by the European Union brought in the various concept of Information Privacy and Security. MGC Global Risk Advisory LLP IT risk advisory team through their leadership paper brings in the importance of data protection.

The European Parliament adopted the General Data Protection Regulation (GDPR) in April 2016, requiring certain classes of companies in accordance with the applicability criteria to protect the personal data and privacy of the European Union ('EU') citizens/ residents for transactions that occur within 28 member states. Tarun Kher, Partner, MGC Global Risk Advisory LLP, brings in his thoughts through his leadership paper.

APPLICABILITY

GDPR compliance is applicable to all companies processing and archiving personal information (including personally identifiable data within social media, photos, email addresses and IP addresses) regarding EU citizens/ residents within EU states, even if such companies do not have a business presence within the EU. The below mentioned companies are required to adhere with GDPR provisions:

- A presence in an EU country;
- No presence in the EU, however the Company processes personal data of European citizens/ residents;
- More than 250 employees; &
- Fewer than 250 employees however 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 for overseeing the data security strategy in cases where Companies process or archive significant volume of personally identifiable information, regularly monitor pertinent data subjects, or are a public entity (except law enforcement authorities, which may be exempt).

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.

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 below mentioned 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;

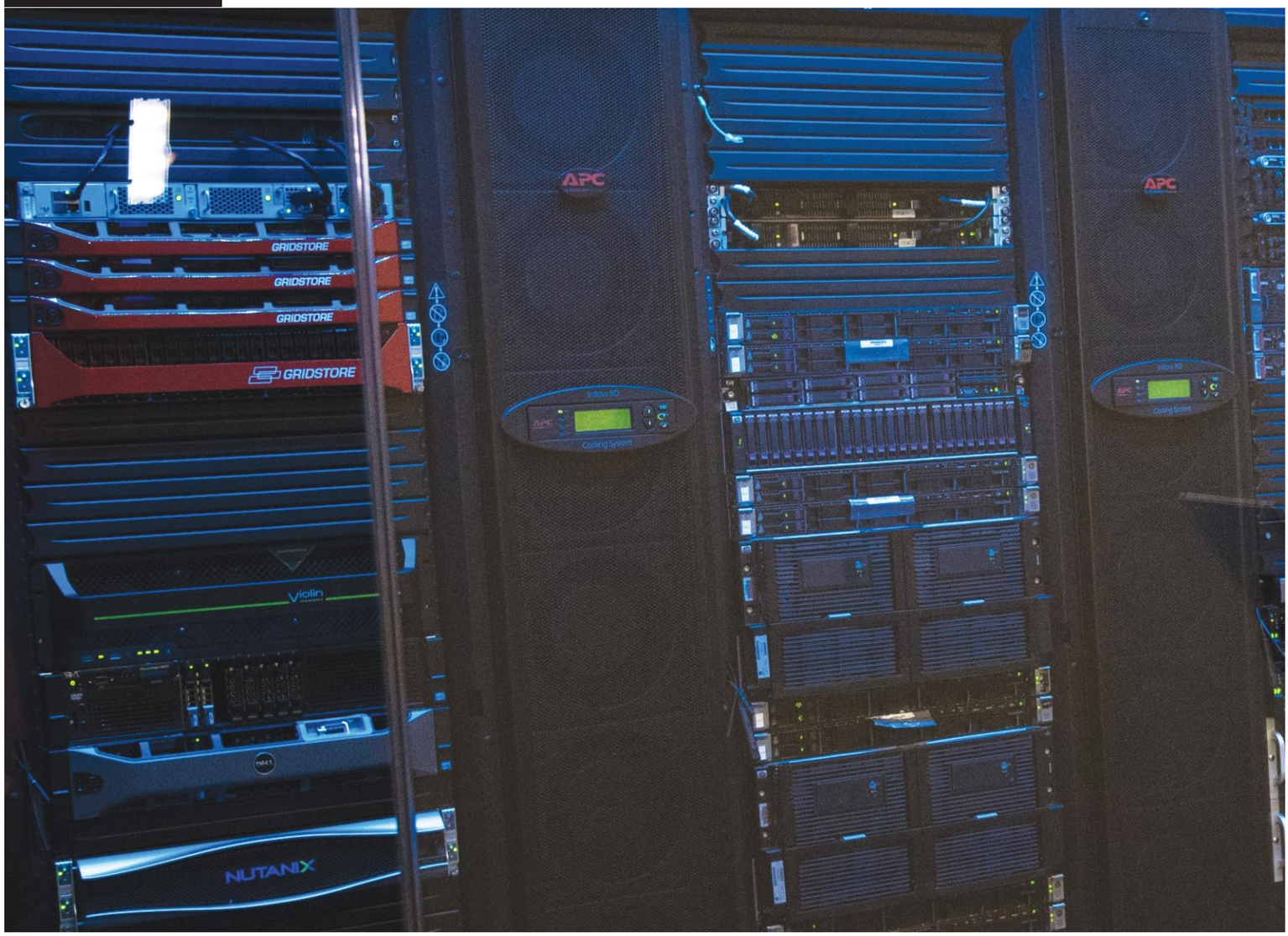
b) Right to be forgotten: includes permanent or on-demand deletion of his/her personally identifiable data, cease further distribution of the data, and demand third parties' restriction on processing of the data.

c) Data breach notification: As a data breach is likely to result in a risk to the rights of data subjects, 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.

d) 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 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.

CONCLUSION DATA PROTECTION IMPACT ASSESSMENTS

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.