The Institute of Internal Auditors Singapore

The General Data Protection Regulation (GDPR) and its impact for Asia

The General Data Protection Regulation (GDPR) is a regulation from the European Union (EU) about data protection and privacy. Under this regulation, organisations which deal with personal data from the EU have to comply with different obligations.

The GDPR came into force on 25 May 2018. As the territorial scope of this regulation extends to organisations that target EU residents, it will impact Singapore-based companies who do business with EU residents.

In addition, both Singapore and Asian companies might, through their contracting partners, be obligated to comply with the GDPR in the light of business entities that may deal with the EU and their residents. In order to adhere to this regulation, affected companies will have to undertake a root and branch review of how they process, handle and govern the personal data obtained from EU residents.

How internal audit can facilitate GDPR compliance?

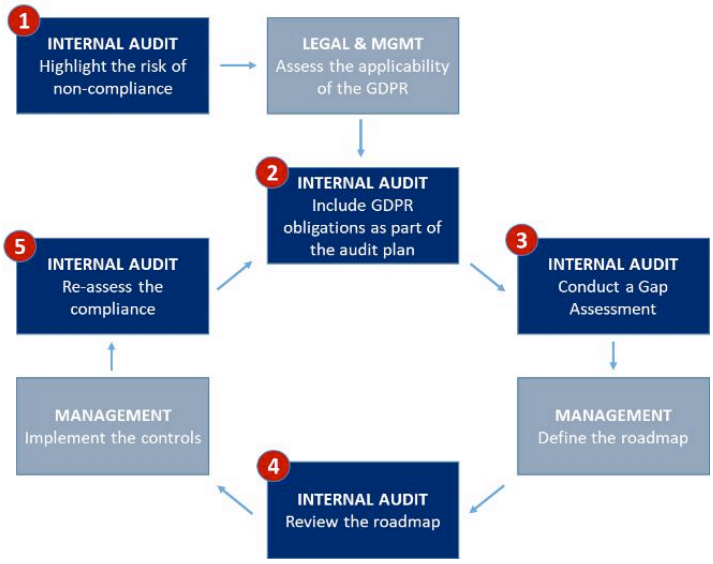
Against this backdrop of developments, this is where internal auditors can play a critical role in ensuring GDPR compliance.

They can highlight the risks of non-compliance, help with the data flow, or identify gaps with the regulation by conducting assessments. Thereafter, risks can be mitigated and appropriate remedial procedures can be put in place.

As a starting point, we have identified a 5-step approach for internal audit departments to consider.

Commonly used GDPR terms:

* Data controller: the entity that determines the purposes, conditions and means of the processing of personal data.
* Data processor: the entity that processes data on behalf of the Data Controller
* Data Protection Officer: an expert on data privacy who works independently to ensure that an entity is adhering to the policies and procedures set forth in the GDPR
* Personal Data: any information related to a natural person or 'Data Subject', that can be used to directly or indirectly identify the person
* Data Subject: a natural person whose personal data is processed by a controller or processor
* Processing: any operation performed on personal data, whether or not by automated means, including collection, use, recording, etc.



1. **Highlighting the risk of non-compliance**

Many organisations are not yet aware that the GDPR is applicable to them. One of the initial initiatives of internal audit should be to escalate to the Board or Risk Committee about the risks that non-compliance pose to the company: hefty fines up to 4% of the global annual turnover, reputational damage, and/or court trials, could significantly harm the organisation.

Once the potential risks are identified, the internal auditor will then have to play a role in providing a certain assurance and awareness to the firm about whether the GDPR will be applicable. This ties in with the internal audit's role to minimise the exposure to risks. If the firm does not comply with the GDPR, it will face serious consequences.

Internal auditors will need to develop knowledge on GDPR and the impact of it on the organisation. Conducting a GDPR gap assessment will identify which obligations the company already complies with, and the extra effort required to achieve full compliance.

2. **Scoping the applicable obligations**

Let's assume the organisation has already identified that the GDPR is applicable and mapped all the processed personal data. Before tackling the GDPR gap assessment, internal auditors play a pivotal role in scoping the sections of the GDPR which are applicable to the firm. This will depend on a few factors including the type of data processed, the engaged data processors and the types of data subjects.

3. **Conducting a gap assessment**

A GDPR gap assessment comprises relevant and applicable GDPR obligations which the company has to adhere to. The key obligations that require specific attention include the following:

a) Data protection officer (DPO) and support force

The appointment of a DPO under the GDPR is mandatory when the organisation is a public authority or body, or when the organisation's core activities consist of processing operations that require regular and systematic monitoring of data or large-scale processing of special categories of data (i.e. sensitive data).

b) Legal basis and lawfulness of processing

In order for processing to be lawful, organisations will have to identify the legitimate basis (e.g. the data subject's consent) to process personal data.

c) Data governance

The GDPR requires strong data governance processes. Through their overseeing role, internal auditors should review, verify and provide recommendations related to data governance initiatives, such as the mapping of data flows, the identification of different types of personal data and the management of access rights.

d) Contractual obligations and data transfers

Article 28 of the GDPR includes a specific list of requirements that a controllers must include in their contracts with their processors (e.g. requirements on retention, access, security or involvement in the regulation compliance.) The internal audit function can verify whether the obligations related to data processing contracts and data transfers are adhered to.

e) Risk assessment and mitigation

Assessing the organisation's unique risk profile and taking appropriate measures to mitigate the security risks allows the company to comply with the GDPR (as part of its requirement on periodic risk assessment) but also to mitigate the risk of data breaches.

f) Data breach notification

The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. When the personal data breach is likely to result in a high risk to the rights and freedom of natural persons, the controller must communicate the personal data breach to the data subject without delay.

g) Documentation of processing activities

Documenting the organisation's processing activities in a granular and meaningful way is now mandatory under the GDPR.

h) Data subject rights

The GDPR sets forth a range of specific data subject rights which can be exercised under particular conditions.

i) Data protection

Based on well-known cybersecurity standards (e.g. ISO, NIST, etc.), internal auditors can verify whether the organisation has implemented sufficient guarantees to secure the personal data.

As the GDPR impacts many activities and functions within a typical organisation, internal auditors should look into the processing activities of the following departments:

1. Marketing, as they collect and use personal data of customers.
2. HR, as they process personal data of personnel.
3. Legal, as they have an overview of relevant regulations that need to be adhered to, and they manage contracts where data protections clauses might need to be included.
4. Procurement, as service providers might need to be GDPR compliant as well.
5. Business and Operations where personal data is involved, as they process, use or report the data.
6. IT, as they are responsible for the protection of the data residing in the organisation's systems.

4. Maturity statement and privacy roadmap review

After conducting the gap assessment, internal auditors can provide insightful viewpoints on which compliance level the organisation should aim for. This maturity statement will be based on the risk appetite and tolerance of the company, and will form the basis of the privacy and data protection framework.

Management will prioritise the gaps identified during the gap assessment, and those will be sequenced into a privacy roadmap whose objective is to ensure compliance with the GDPR.

Internal auditors can then review the privacy roadmap to ensure that sufficient actions have been planned to comply with the different obligations

5. Periodic audit assessment

Through periodic assessments, the internal audit function verifies to governing bodies that gaps have been rectified. These audits demonstrate to regulators that applicable GDPR obligations have been complied with.

Moreover, recurring internal audits will enable the key stakeholders (Board of Directors, Risk Committee, Chief Operating Officer, Data Protection Officer, Chief Information Officer, etc.) to keep track of the effectiveness of the measures implemented, to reflect whether the organisation is on track with the privacy roadmap, and to highlight which obligations are still outstanding.

The GDPR has ushered in a raft of changes that would mean transformation of a company's risk management procedures. It is certainly an area where companies need to manage carefully given the risks and liabilities involved. More than any time, internal auditors also play an instrumental role in a company's journey towards GDPR compliance. It is time for them to step up and step into the spotlight.