June 2018

Risk and Performance Quarterly

GDPR: An Opportunity for Internal Auditors to Lead the Focus on Data Protection

By Mark D. Bednarz, CPA, CISA, CFE, Partner and Lawrence A. Baye, CMC, CISA, Principal

The European Union (EU)'s General Data Protection Regulation (GDPR) has awakened us to the importance of securing our data and to be mindful of an individual's privacy. For organizations that must adhere to GDPR, not only will they be subject to specific technical, administrative and legal requirements but also potential liability. Whether or not a specific organization must comply with the regulation, it has a responsibility to properly secure and control the use of personal data. Internal auditors should take this opportunity to assess the risks related to personal and other sensitive data (i.e., intellectual property).

For all organizations, there are benefits in implementing data protection controls and performing a data protection internal audit. The audit will help ensure that the organization has the appropriate IT controls in place, identify the location of personal and sensitive data, improve data quality, limit the amount of data collected from individuals, and restrict access to data.

Internal auditors should engage management in assessing existing controls around data protection. Prior to assessing the organization's data protection needs, internal audit should inquire whether management has taken the necessary steps in determining whether the organization is impacted by the regulation. The compliance requirements are backed by heavy financial penalties.

In recent years, IT departments and internal auditors have been focusing on network security, logical security and access management, such as firewalls, intrusion detection, anti-virus, password complexity rules and removing terminated users. These controls will directly or indirectly support data privacy. GDPR and data protection assessments, however, go beyond cybersecurity. Internal audit is advised to begin to shift from a system-driven security approach to one where the focus is on data-driven security.

Some of the GDPR data management principles and requirements that should be considered include:

- Data minimization – the practice of collecting the least amount of data needed to perform the task or service.
- Privacy by design – the concept of embedding privacy into the development and operation of IT systems and business practices. Too often in the rush to implement a new technology, little time is spent thinking through the ramifications of collecting, analyzing and/or disseminating sensitive information
- Pseudonymization – the process of replacing most identifying fields with data records with artificial identifiers.

As a part of a cybersecurity or incident management audit, internal auditors evaluate how incidents are identified, logged, tracked, escalated, and addressed. Internal auditors can expand their cybersecurity or incident management audit programs by incorporating elements from GDPR, which include defining personal data breaches and the response time in notifying government agencies and impacted individuals.

The data protection regulation will help broaden the understanding of data protection for both management and internal audit. For example:

- Article 4 of the Regulation defines personal data as “any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.”
- Article 9 expands the definition of personal data by including genetic and biometric data, which uniquely identifies an individual. GDPR refers to this type of information as “special categories of personal data.”
- Article 7 focuses on obtaining consent from the individual/data subject. Internal audit should inspect policies, procedures, notifications and forms related to personal and other sensitive data. The policies should cover obtaining consent, providing choices where appropriate, and focusing on only collecting personal data that is adequate and relevant. In order for consent to be effective, the organization’s current technology should be evaluated to ensure it is adequate in managing consents.

Focusing more on internal audit rather than implementing GDPR requirements, internal audit should take a risk-based approach in creating their audit program by defining the scope, and identifying, analyzing, evaluating and monitoring risks. While the primary goal is to secure data, it is only achievable if management implements the right set of controls to secure hardware, software, network components and supporting assets (i.e., paper documents, individuals).

When considering the risks relevant to data protection, internal audit should identify internal and external factors, such as regulations, contractual agreements with service providers, existing internal controls, security threats and business factors. To identify risks, internal audit should classify risk sources, assets (including information, personal data, systems, etc.), threats and weaknesses, as well as possible impact and data protection risks.

As internal audit engages management in performing a data protection audit, the team should determine — with the help of management — the processes, departments, technology and outsourced providers that “touch” sensitive data. Depending on the size of the organization, internal audit may need to conduct surveys or hold workshops in order to flush out the departments that collect and manage personal and other sensitive data.

A data flow diagram is an excellent tool for internal audit to understand the flow of personal and other sensitive data. As internal audit follows the flow of data, they should identify information technology, compliance and manual controls that are already in place. Organizations that have insight into their data flows are in a better position to understand the impact of a data breach.

Performing data mapping may be challenging for some teams as they attempt to identify departments that utilize personal and other sensitive data, inventory what data is collected, locate where the data is stored, assess the sufficiency of technical and organizational safeguards, and understand the legal and regulatory obligations at the different locations. After internal audit evaluates the results from their fieldwork, which include the data flow diagrams, walkthroughs, policies, procedures, notices and forms, and internal control system, the internal auditors should consider the impact and likelihood of unauthorized access, unwanted modifications and loss of personal and other sensitive data. After classifying the severity of the risk, the internal auditors will be able to provide meaningful recommendations in addressing data protection risks.

One of the GDPR regulator expectations is the creation of a Data Protection Impact Assessment (DPIA), which helps identify and address risks at an early stage by analyzing how the proposed methods will

mitigate identified risks. In the case of GDPR, there is a legal obligation to perform a DPIA, where processing — in particular using new technologies — and taking into account the nature and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons.

One of the recommendations that should be presented in the internal audit report is conducting a DPIA when projects (i.e., new IT system, data sharing initiative, legislation, etc.) are initiated that impact personal or other sensitive data. After the project lead or IT complete the DPIA, the executive sponsor should evaluate the residual risks to assess whether to move forward with the project, determine (a) if the assessment was sufficient and complete, and (b) if existing internal controls are operating effectively so the residual risks are at acceptable levels or if they require additional controls.

Data protection and governance are not new concepts, but the enactment of GDPR raises awareness of the importance of safeguarding personal information. Internal audit should spearhead the initiative because shining a light on protecting the privacy of personal data not only builds trust but also reduces the level of reputational and regulatory risk.

Contact Us

If you have any questions or comments about GDPR or would like our assistance in implementing its requirements, please contact any of the following individuals or your PKF O'Connor Davies engagement team:

Mark D. Bednarz, CPA, CISA, CFE
Partner
mbednarz@pkfod.com

Lawrence A. Baye, CMC, CISA
Principal
lbaye@pkfod.com

Thomas J. DeMayo, CISSP, CISA, CIPP/US, CRISC, CEH, CHFI, CCFE
Principal
tdemayo@pkfod.com

About PKF O'Connor Davies