Assurance Considerations for Ongoing GDPR Conformance

If you have reviewed my bio, you are aware that I have more than 30 years of experience in all aspects of information systems. I started out as a BASIC programmer working for a small software company where many of the customers were still using computers that ran the CP/M[1] operating system with 8-inch floppy disks. Computer literacy and the accompanying controls (e.g., encryption) were only in their infancy, so, for testing purposes, we often requested that copies of clients' data were sent to us in the post. We once received a photo copy of a disk. On another occasion, the disks were folded in half so that they would fit in an envelope.

I, and the industry at large, have been through several projects since then including the Millennium Bug (Y2K), the Euro Conversion and, most recently, the EU General Data Protection Regulation (GDPR). However, there is a significant difference between GDPR and the other projects. While the former had hard deadlines, the latter is something with which our enterprises must continue to comply.

So, now, how can we mitigate the ongoing risk of nonconformance? How can we ensure that the newly developed GDPR processes and procedures transition into day-to-day practices and become business as usual?

Early in 2018, ISACA® released *Implementing the General Data Protection Regulation*.[2] Annex 1 of the document defined nine core GDPR processes (**figure 1**) in a COBIT® 5-like process model to form a data protection management system (DPMS). These processes should be mapped to your enterprise's existing GDPR processes and reviewed from an assurance perspective.

DPP1—Maintain Data Governance

The governing processes should enable all associates and other internal and external stakeholders to rely on a defined set of principles, policies and procedures that clearly define and explain how personal data may be processed and how senior management and other leadership functions support related activities.[3] Assurance concerns include:

- Is there a *data protection and privacy governance framework*, for example, policies describing the personal data universe, purposes for processing, limitations and controls?
- Is there a *data processing register*, for example, a processing life cycle from initial data acquisition to data deletion?

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA® website (*www.isaca.org/journal*), find the article and click on the Comments link to share your thoughts.

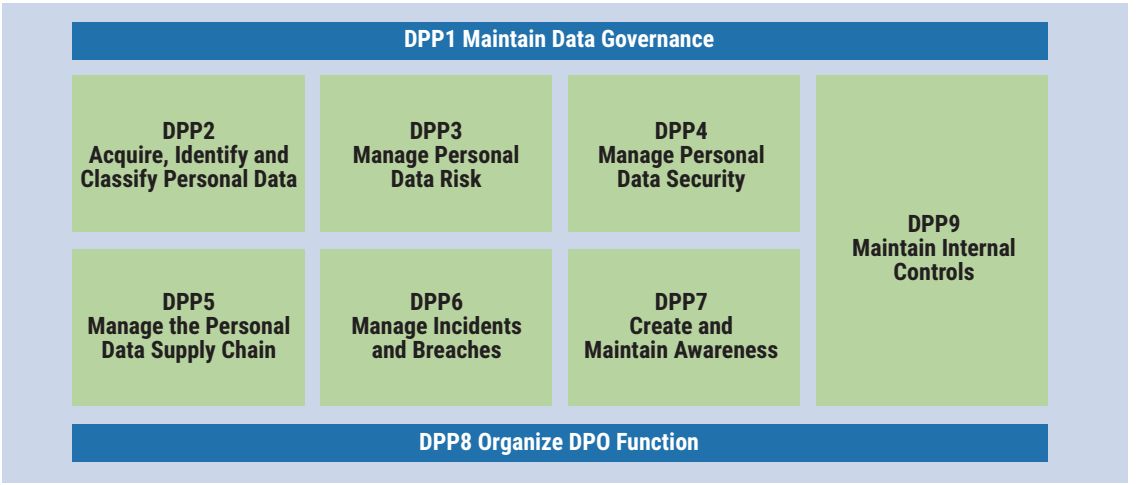
https://bit.ly/2G3g9Di

Ian Cooke, CISA, CRISC, CGEIT, COBIT Assessor and Implementer, CFE, CIPM, CIPT, CPTE, DipFM, ITIL Foundation, Six Sigma Green Belt
Is the group IT audit manager with An Post (the Irish Post Office based in Dublin, Ireland) and has 30 years of experience in all aspects of information systems. Cooke has served on several ISACA® committees and is a past member of ISACA's CGEIT® Exam Item Development Working Group. He is the topic leader for the Audit and Assurance discussions in the ISACA Online Forums. Cooke supported the update of the *CISA® Review Manual* for the 2016 job practices and was a subject matter expert for the development of ISACA's CISA® and CRISC™ Online Review Courses. He is the recipient of the 2017 John W. Lainhart IV Common Body of Knowledge Award for contributions to the development and enhancement of ISACA publications and certification training modules. He welcomes comments or suggestions for articles via email (Ian_J_Cooke@hotmail.com), Twitter (@COOKEI), LinkedIn (*www.linkedin.com/in/ian-cooke-80700510/*) or on the Audit and Assurance Online Forum (*engage.isaca.org/home*). Opinions expressed are his own and do not necessarily represent the views of An Post.

Enjoying this article?

- Read *How to Audit GDPR*. *www.isaca.org/how-to-audit-GDPR*
- Learn more about, discuss and collaborate on audit and assurance ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

Figure 1—Data Protection and Privacy Process Model



Source: ISACA®, *Implementing the General Data Protection Regulation*, USA, 2018. Reprinted with permission.

- Are there *binding corporate rules (BCRs)* in place (if required)? Are these regularly validated?
- Are *rules for consent* defined (e.g., how do data subjects withdraw consent)?
- Are *rules for data subject requests* defined (e.g., are there independent reviews of requests by the data protection officer [DPO] function)?
- Are there *rules for managing data subject complaints* (e.g., are gaps or weaknesses leading to the complaint reviewed for improvement opportunities)?
- Is there a process to ensure impartial oversight (e.g., is the DPO function reviewed by internal or external audit)?

DPP2—Acquire, Identify and Classify Personal Data

Enterprises must provide a robust process that ensures GDPR-conformant processing and efficient data management. This process should also establish a defined and measurable life cycle for personal data, taking into account the principle of data minimization.[4] Assurance concerns include:

- Is the *data life cycle managed* (e.g., has information asset classification, including protection levels, been defined)?
- Have all *personal data been identified*?
- Have all *personal data been classified*?
- Is a *personal data register* maintained (e.g., have personal data been documented in terms of their metadata)?
- Are *special categories of data* managed (e.g., identification and controls of any processing of data belonging to one or more of the special categories)?
- Is the *right of erasure (right to be forgotten)* managed?

> "PERSONAL DATA PROCESSING IS SUBJECT TO A NUMBER OF PREDEFINED RISK SCENARIOS THAT MUST BE IDENTIFIED, EVALUATED AND TREATED IN AN ADEQUATE AND APPROPRIATE MANNER."

DPP3—Manage Personal Data Risk

Personal data processing is subject to a number of predefined risk scenarios that must be identified, evaluated and treated in an adequate and appropriate manner. The potential impact of these

risk factors must be assessed and analyzed in view of existing risk mitigation measures.[5] Assurance concerns include:

- Are *risk evaluations* conducted to identify events and threats that might lead to materialized risk?
- Are *Data Protection Impact Assessments (DPIA)* conducted?
- Are the *identified risk factors* treated based upon the evaluation and impact?
- Will the identified *risk scenarios* be regularly reevaluated?

> "MAINTAINING DATA PROTECTION AND PRIVACY AS FUNDAMENTAL VALUES WITHIN AN ENTERPRISE REQUIRES AWARENESS AND ONGOING INFORMATION AND EDUCATION."

DPP4—Manage Personal Data Security

Personal data processing requires adequate and comprehensive security around the information assets in scope. As personal data—and personally identifiable information (PII) in the wider sense—represent a significant business and financial value, they should be treated accordingly and assigned an adequate level of protection in terms of confidentiality, integrity and availability (CIA).[6] Assurance concerns include:

- *Anonymization and pseudonymization* of the data
- *Encryption* of the data (where applicable)
- *Resilience* of data
- *Managing access* to the data
- *Testing and assessing* the data security on a regular basis

DPP5—Manage the Personal Data Supply Chain

Where personal data are processed by more than one organization, the supply chain across all controllers and processors must be managed and controlled in accordance with GDPR. The management process, therefore, includes all controllers (jointly or separately) and any subprocessors handling personal data.[7] Assurance concerns include:

- The identification of *primary controllers, joint controllers and data processors*
- *Managing of subprocessors* including evidence of GDPR conformance
- *Managing processing agreements*
- Has the enterprise applied its own data protection impact assessment (DPIA) approach to all parts of the *supply chain*?
- Has the enterprise ensured that *internal controls at a processor or subprocessor* are as effective as its own controls?

DPP6—Manage Incidents and Breaches

Data protection-related incidents and breaches must be reported in line with GDPR. This includes notification of supervisory authorities and communications with data subjects actually or potentially affected by the breach.[8] Assurance concerns include:

- Does the *breach notification process* meet GDPR requirements (e.g., within 72 hours)?
- Does the *notification of data subjects* satisfy the mandatory GDPR requirements?
- Is an *incident and crisis management* process in place?
- Are processes in place to *secure evidence* and for substantiating or defending against claims resulting from the incident or breach?

DPP7—Create and Maintain Awareness

Maintaining data protection and privacy as fundamental values within an enterprise requires awareness and ongoing information and education.

The awareness process supports all other processes by explaining, communicating and reinforcing both GDPR requirements and good practice.[9] Assurance concerns include:

- Is a process in place to *maintain enterprisewide awareness*?
- Is a process in place to ensure that the *required skills and education* are available to the enterprise?
- Is a process in place to provide *ongoing learning opportunities* to reinforce the key GDPR messages?

DPP8—Organize DPO Function

The GDPR mandates a DPO as an individual or as a function. A process is needed to ensure that once established, the DPO performs regular tasks and interacts with other parts of the enterprise. In doing so, the DPO must further ensure conformance with laws and regulations and, specifically, with GDPR.[10] Assurance concerns include:

- *Managing the DPO function* (e.g., are organizational structures in place?)
- Have a *budget and resources* been allocated?
- Are *organizational interfaces* in place (e.g., to allow the function to interact with other parts of the enterprise)?
- Is formal *internal and external reporting* in place?
- Are *external, contracted GDPR processes* managed?

DPP9—Maintain Internal Controls

The process of maintaining internal controls over personal data processing should be fully aligned with the general system of internal controls operated by the enterprise.[11] Assurance concerns include:

- Are data *acquisition controls* (e.g., consent or legitimate/public interest) maintained?
- Are the data subject to controls that ensure *lawful* processing and adherence to the defined purpose?
- Are the *data at rest* (i.e., stored or archived) subject to controls for confidentiality, integrity and availability?
- Are *data deletion controls* linked to the data processing life cycle to ensure timely deletion?
- Are personal data processing, storage, deletion and any other uses subject to *permanent monitoring*?
- Is personal data processing *reviewed in an independent and impartial manner*?

Audit Program

In October 2018, ISACA released a GDPR Audit Program[12] that builds upon these assurance considerations, defining the related control objectives, the necessary controls and documenting the suggested testing steps. This can be used to confirm conformance with the GDPR.

Conclusion

Regulations such as GDPR have, quite rightly, made it unacceptable to send unencrypted personal information in the post. Indeed, the fines for doing so are very onerous. Now that GDPR is here, enterprises face the challenge of transitioning the identified processes into day-to-day practices while also seeking assurance that they are in conformance and, as no doubt GDPR will evolve, are also subject to continual improvement. The data protection management system (DPMS) and the related audit program enables this while further facilitating the definition of measurable indicators and maturity modeling among others.

Author's Note

It should be noted that the *Implementing the General Data Protection Regulation*[13] guide also defines subprocesses for each of the processes defined in **figure 1**. They have not been reproduced here due to space constraints. Processes exist for all items that have been italicized.

Endnotes

1 Delony, D.; "CP/M: The Story of the OS That Almost Succeeded Over Windows," Techopedia, 15 May 2015, *https://www.techopedia.com/2/31154/software/cpm-the-story-of-the-os-that-almost-succeeded-over-windows*
2 ISACA, *Implementing the General Data Protection Regulation*, USA, 2018, *www.isaca.org/Knowledge-center/Research/ResearchDeliverables/Pages/Implementing-the-General-Data-Protection-Regulation.aspx*
3 *Ibid*. p. 62
4 *Ibid*., p. 65
5 *Ibid*., p. 68
6 *Ibid*., p. 70
7 *Ibid*., p. 75
8 *Ibid*., p. 76
9 *Ibid*., p. 78
10 *Ibid*., p. 80
11 *Ibid*., p. 82
12 ISACA, *GDPR Audit Program*, USA, 2018, *www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/GDPR-Audit-Program.aspx*
13 *Op cit Implementing the General Data Protection Regulation*