FEATURE

Reporting on GDPR Compliance to the Board

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/2QEFcQR

In preparing for compliance with the EU's General Data Protection Regulation (GDPR), a multinational organization with exposure to the European Union sought a simpler way to affect the complexity of the compliance matters facing the organization. In particular, they sought ways to assess compliance progress for presentations to the board and senior leadership team (SLT) so that the board and management could readily understand the compliance requirements and, subsequently, appropriately react to them.

They identified eight knowledge areas representing the GDPR's span against which the management team would be required to report at each board meeting. They are a possible starting point for those facing a similar governance requirement in their own organizations. These may be especially valuable given that many organizations that should have been compliant by 25 May 2018 seem to not be yet.[1]

Today, there are many different GDPR assessment methods available to suit many different purposes, including the ISACA®-CMMI GDPR Assessment.[2] The framework in this article was created specifically for the purpose of reporting to the board. It came about when a board director, discussing the topic of GDPR compliance, suggested that all that was required for board reporting was to document exposure and the relevant risk controls. GDPR is, however, multifaceted and complex, and a single answer would not provide the board with sufficient insights in a context where privacy is deemed a basic human right, not simply a barrier to doing business.

Guy Pearce, CGEIT
Has served on private and public boards in banking, financial services, retail and a not-for-profit over the last decade. He also served as chief executive officer of a multinational retail credit business and has published numerous articles on various aspects of governance and risk. He is an independent consultant specializing in strategy, governance and risk.

The Multidisciplinary Nature of GDPR Compliance

GDPR, which served to synchronize Europe's data privacy regulations and to empower EU natural persons with respect to their data privacy, went into effect on 25 May 2018. Whereas many may think that the organizational impact of GDPR is on the privacy, legal and compliance fronts, the reality is completely different. Indeed, for most affected medium to large organizations, achieving compliance impacts most of the C-suite or their functional equivalents. GDPR is now recognized as a multidisciplinary issue (**figure 1**).[3]

The board's role is to ensure compliance with the regulation to mitigate the risk of incurring financial penalties for noncompliance. While the maximum penalty for noncompliance is up to 4 percent of global revenue, there are organizations that could sustain this financial penalty. However, there are others—many of them smaller businesses—that may not be able to survive a penalty of this scale. They would, thus, be subject to sustainability risk. It is also the board's responsibility to mitigate the reputational risk of falling foul of the new regulation. A framework for board and SLT reporting is recommended (**figure 2**).

For clarity, an operating model (**figure 2**) enables the translation of strategic intent into operational capabilities.[4] Practitioners may be familiar with the basic organizational capabilities such as talent (people), processes and technology. While there are

Figure 1—Examples of the Implications for the C-Suite of Becoming GDPR Compliant		
Role	**Implication**	**Examples of Relevant GDPR Sections**
Chief executive officer (CEO)	Accountable for enterprise risk, including reputation, compliance and operational risk	The CEO is ultimately responsible for risk.
Chief financial officer (CFO)	Financial penalties	Up to €20 million or 4 percent of global revenue; see recitals 148 and 150, and article 83
Chief information officer (CIO)	Systems changes and IT governance	Data portability in a structured, commonly used machine-readable format (article 20).
Chief data officer (CDO)	Data changes and data governance	Data rectification and completeness (personal data needs to be accurate and kept up to date [article 5])
Chief marketing officer (CMO)	Consent	"Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her." (article 32)
Chief operations officer (COO)	Rights of the data subject	The right not to be subject to automated decisions (article 22)
Chief HR officer (CHRO)	Code of conduct	Article 40
• Note that there could be overlap		

Figure 2—The Objectives of the Reporting Framework	
Objectives	**Comments**
Create a classification framework that is easy to understand by all board members and members of the SLT.	To have a simplified communication framework rather than reporting on compliance with potentially 99 GDPR articles and 173 recitals
Create a common understanding of the major operating model implications of various parts of the regulation.	For the board to perform oversight of the capacity and capability requirements of the operating model implications of compliance; primary, secondary and tertiary operating model constructs were identified for each relevant part of the regulation
Create a simple view of the progress being made against each category.	Performance reporting against plan and against prior reporting period (where was progress made since last period)

more—such as leadership and insights—this article focuses on these three.

Classification

Not only do the 99 GDPR articles not readily lend themselves to simple classes for reporting purposes, there are aspects of the GDPR that are not relevant to all businesses, such as articles for healthcare or the public sector. Eight classes with larger organizational applicability were identified.

Importantly, fulfilling the requirements encapsulated within each class has specific operating model implications. An operating model is an organizational construct that enables the provision of value to the organization's stakeholders. While there could be many different elements of an operating model in an organization, the common elements are people, process and technology.[5] Since regulations impact how organizations operate, it is important to analyze regulatory changes from an operating model context.

> "SINCE REGULATIONS IMPACT HOW ORGANIZATIONS OPERATE, IT IS IMPORTANT TO ANALYZE REGULATORY CHANGES FROM AN OPERATING MODEL CONTEXT."

> “...[T]O ACHIEVE THIS LEVEL OF UNDERSTANDING REQUIRES AN EXTENSIVE ANALYSIS OF THE ORGANIZATION’S CURRENT STATE, A QUANTUM OF WORK NOT TO BE UNDERESTIMATED.”

The elements of an operating model are interdependent. In many cases, though, one of the elements is a driver of that interdependency. For example, consider an organization that wants to improve efficiencies by automation. If the organization has documented processes, then those processes would be the primary driver of automation. If it does not, then the staff would be consulted in a facilitated session to draw out a process map, which could then have technology applied to it. In the first case, processes are the driving operating model construct, while in the second case, people are the driving operating model construct. Technology can also be a driver. For example, if the need is to create a record of transactions with multiple points of failure, a distributed system (rather than a centralized system) may be the driving operating model construct.

While an assessment of the primary operating model implication of each class is suggested in the figures that follow, this may differ for organizations in different states of maturity and that have different business drivers.

Note also that for the purposes of this discussion, the content of the classes do not strictly follow the regulation’s order of things; rather, content is grouped together to facilitate reporting. The following subsections describe the class types.

Rights of the Data Subject

This is possibly the most important class, given that the GDPR was written to protect these rights. Identifying what needs to be done to protect these rights needs to be articulated properly. In particular, Chapter 3 of the GDPR documents the rights of the data subject (**figure 3**), in other words, the rights of those about whom an organization keeps data.

As a guide to reading the figures, using **figure 3** as an example, to achieve the requirement of the right of a data subject to access data about them, the primary organizational implication would be to develop a process to fulfill this. Whether the process would be partially or fully automated by the business is, therefore, a secondary operating model implication. Another organization might already have a process, so its primary driver might be technology (automation).

It is very important to note that to achieve this level of understanding requires an extensive analysis of the organization’s current state, a quantum of work not to be underestimated.

Achieving compliance in this class has significant technology implications, as seen in the right column of **figure 3**. Meeting the requirements of this class could incur significant cost and could take

Figure 3—Basic Natural Person Rights Under GDPR

Rights	Primary Operating Model Driver
To access their data	Process
To correct their data	Process
To be forgotten (erasure of personal data)	Technology
To request that you stop processing their data	Technology
To not be subject to automated decision-making	Technology
To be informed about how data about them are collected and processed and how the data will be used	People
To data portability, i.e., data can be exported in machine-readable format to be used elsewhere	Technology

considerable time to achieve, especially in legacy environments.

Obligations of the Data Controller as an Organization
The next most significant area concerns data controllers, who are the legal or natural persons—operating either independently or jointly—who decide the purpose of the processing of personal data. **Figure 4** details their obligations.

Personal data can only be processed under certain conditions, one of them being receiving the freely given consent of the data subject. Other situations where the processing of personal data is allowed are legal obligations, public interest, contracts, legitimate interest and the vital interests of the data subject.

While freely given consent is a GDPR requirement of relevant organizations, in Canada, the privacy commissioner has begun enforcing guidelines for obtaining meaningful consent for all Canadian private-sector organizations effective on 1 January 2019.[6]

Obligations of the Data Processor
A data controller can contract a data processor to process personal data as a service to the controller (outsourced data processing). Chapter 4 of GDPR documents the obligations of data processors as per **figure 5**.

Note that not every organization outsources all or even part of their data processing.

Figure 4—Some Obligations of Data Controllers

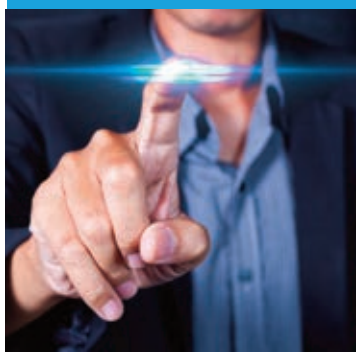
Obligations of the Data Controller	Primary Operating Model Driver
Appropriate consent	Technology
Privacy impact assessment	People
Maintaining a record of processing	Technology
Data protection by design and by default	Technology
Ensuring that data processors are compliant	Process
Appointing a data protection officer if justified	People
Taking due care when transferring data out of the EU	Process
Ensuring security appropriate to the level of data processing	Technology
Breach notification both to the relevant authority and to the affected data subjects in 72 hours	Process

Figure 5—Some Obligations of Data Processors

Obligations of the Data Processor	Primary Operating Model Driver
Maintaining a record of processing	Technology
Data protection by design and by default	Technology
Ensuring security appropriate to the level of data processing	Technology
Requiring written data processing instructions from the controller	People
The processor needs to be governed by means of a contract from the controller	People
Cannot engage another processor without written consent from the data controller	People
Providing breach notification both to the relevant authority and to the affected data subjects in 72 hours	Process

Enjoying this article?

- Read *Maintaining Data Protection and Privacy Beyond GDPR Implementation*. *www.isaca.org/Data-Protection-Beyond-GDPR*
- Learn more about, discuss and collaborate on information security management in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*



> PRIVACY BY DESIGN HAS IMPLICATIONS FIRST AND FOREMOST FOR PEOPLE, ALTHOUGH ITS IMPACT SHOULD ALSO BE FELT STRONGLY IN THE PROCESS AND TECHNOLOGY DOMAINS.

Record Keeping

Quite possibly one of the most important parts of the regulation from an audit perspective, GDPR requires controllers and processors to maintain records of their processing (article 30 and recitals 13 and 82), particularly if they employ more than 250 staff. Good record keeping enables a demonstration of compliance. **Figure 6** outlines these requirements.

If an organization employs fewer staff, the record keeping requirement is reduced (not eliminated), except if their processing poses a risk to the rights and freedoms of the data subjects, the processing is frequent or the processing includes certain special categories of data.

Privacy by Design

> *Privacy by design … advances the view that the future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must ideally become an organization's default mode of operation.*[7]

Little speaks more to this than beginning with a code of conduct. Indeed, London-based global telecommunications giant Vodafone Group put it this way:

> *The protection of personal data is one of our highest priorities and is central to the Vodafone Code of Conduct that everyone who works for us (or on our behalf) must follow.*[8]

While GDPR article 40 speaks of a code of conduct, it seems specific to "associations and other bodies representing categories of controllers or processors."[9] Additionally, every organization should have a code of conduct.[10] It should express the organization's expectations of its staff in protecting the privacy of data subjects.

Privacy by design has implications first and foremost for people, although its impact should also be felt strongly in the process and technology domains.

Data Protection by Design and by Default

GDPR article 25 requires that data processing integrates technical and organizational safeguards to meet the requirements of GDPR and to protect the rights of data subjects from the outset.

For example, GDPR speaks of pseudonymization as a key measure to ensure that personal data are de-identified (design), while data protection by default could be interpreted as ensuring that the least privileged level of access is the default setting for all users.

Figure 6—Key Record Keeping Requirements

Records	Primary Operating Model Driver
Data mapping	Process
Data inventory (e.g., application book of record)	Technology
Able to demonstrate consent	Technology
Required for organizations employing 250 or more people	Technology
Processor needs to use records to be able to show compliance	Technology
Controller needs to be able to demonstrate that processing was performed in terms of Article 5.1	Technology
Changes to processing to be accompanied by a data privacy impact assessment (DPIA), which can be used to demonstrate compliance	People
Controller needs to use technological and organizational measures to ensure that it can show compliance	Technology
If a breach is not reported in 72 hours, the controller or processor must show why the rights of data subjects are not at risk	Technology

Data protection by design and by default has significant implications for the technology dimension of an organization's operating model. Interestingly, given that the GDPR is a privacy regulation, the requirement for data protection by design and by default within the regulation suggests a complementary relationship between security and privacy.

Data Governance by Design

There are requirements expressed within GDPR that are best classified as data governance requirements. For example, the requirements for data accuracy and restitution fall within the data quality knowledge area of Data Management Association International (DAMA) *Data Management Body of Knowledge V2 (DMBOK)*.[11] Updates to personal data in production systems must be strictly governed (assuming such updates are possible) if they are not performed by means of the authorized production applications.

The primary operating model construct impacted is technology, albeit with strong (policy and) process components and strong people (roles and responsibilities) components.

Privacy Commissioner

Privacy commissioners protect and promote the privacy rights of natural persons. The extent of this differs by jurisdiction. Where a data privacy impact assessment of a new form of processing shows the risk to data subjects to be high, it must be communicated to the privacy commissioner (article 36). For consistency, this must be performed in the context of a strong process.

Communicating a breach to the privacy commissioner should be by a strong process performed in conjunction with the corporate communications department to ensure consistency between the message communicated to affected natural persons after a breach and the notification to the privacy commissioner.

Bringing It All Together

With the purpose of all this work having been to create a framework to assess the level of compliance, **figure 7** shows the view-on-a-page of the organization's progress toward compliance.

At a glance, areas of progress from the prior period by class can be identified, along with deficient progress to plan (risk). As a governance construct, part of the reporting includes expectations of delivery for the next period, performance against which can be assessed at that reporting period.

> "THE UTILITY OF A SINGLE-PAGE VIEW FOR BOARD REPORTING PRESENTING THE CURRENT STATE OF GDPR COMPLIANCE, ESPECIALLY AS A WORK IN PROGRESS, CANNOT BE UNDERESTIMATED."

Limitations and Lessons

These findings reflect a perspective of board reporting for an organization in a given state of GDPR compliance maturity. Other organizations in different states of maturity may find different classes and different elements within those classes to be more suitable.

The utility of a single-page view for board reporting that presents the current state of GDPR compliance, especially as a work in progress, cannot be underestimated. However, the only way to truly assess GDPR compliance as an end state is by means of an audit against every relevant article within the regulation, with exceptions reported to the audit committee and then to the board.

A lesson learned is that there are a variety of GDPR assessment frameworks available, with some differences between them driven by the requirements of the impacted organizations, while others cover full compliance, elements of which

Figure 7—Report on a Page—Examples of Elements That Could Appear on a Senior Management or Board Report

As of Month/Year	Operating Model Progress	Progress to Plan	Prior Period Progress
Rights of the data subject	Statement of key achievements past period Statement of key risk factors and controls Statement of key achievements expected next period	↗	→
Obligations of the data controller	Statement of key achievements past period Statement of key risk factors and controls Statement of key achievements expected next period	↗	→
Obligations of the data processor	Statement of key achievements past period Statement of key risk factors and controls Statement of key achievements expected next period	↗	↗
Record keeping	Statement of key achievements past period Statement of key risk factors and controls Statement of key achievements expected next period	↘	→
Privacy by design	Statement of key achievements past period Statement of key risk factors and controls Statement of key achievements expected next period	↘	→
Data protection by design and default	Statement of key achievements past period Statement of key risk factors and controls Statement of key achievements expected next period	↗	↗
Data governance by design	Statement of key achievements past period Statement of key risk factors and controls Statement of key achievements expected next period	↘	→
Privacy commissioner	Statement of key achievements past period Statement of key risk factors and controls Statement of key achievements expected next period	→	↗

Arrow Color	Progress to Plan	Prior Period Progress
Green	Ahead of schedule	There is progress since the prior reporting period.
Yellow	On schedule	There is no progress since the prior reporting period.
Red	Behind schedule	N/A

Note: Actual content is client sensitive and is not shown.

may not be applicable to all organizations. What is more important is that the organizational conversation is guided beyond mere mechanical regulatory compliance and operating model impacts. Yes, there is a sensitivity to all this; helping the organization understand that it is about the rights of the data subjects—human beings—and realizing that members of the organization are those very human beings, if not now under GDPR, then under the updates to privacy regulations in their own jurisdictions that are sure to follow. Ultimately, it is conceivable that business incentives such as the culture change around data can outweigh the regulatory requirements for GDPR compliance.

Endnotes

1 Vigliarolo, B.; "Report: 60% of Companies Likely to Miss GDPR Compliance Deadline," *TechRepublic*, 17 April 2018, *https://www.techrepublic.com/article/report-60-of-companies-likely-to-miss-gdpr-compliance-deadline/*

2 ISACA, ISACA-CMMI GDPR Assessment, March 2018, *http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/ISACA-CMMI-GDPR-Assessment.aspx*

3 EY, *GDPR: Lessons Learned*, 2016, *https://www.ey.com/Publication/vwLUAssets/ey-gdpr-lessons-learned/$FILE/ey-gdpr-lessons-learned.pdf*

4 Murphy, A.; J. Kirwin; K. A. Razak; *Operating Models*, EY, 2016, *https://www.ey.com/publication/vwluassets/operating-models/%24file/operating-models.pdf*

5 Deloitte, "Target Operating Model—TOM," *https://www2.deloitte.com/lu/en/pages/strategy/solutions/target-operating-model.html*

6 Freedman, B.; K. McNeill; "Canada: Preparing for Compliance With New Privacy Consent Guidelines," Borden Ladner Gervais LLP, 17 September 2018, *www.mondaq.com/article.asp?articleid=737060&email_access=on&chk=2469018&q=1731958*

7 Cavoukian, A.; *Privacy by Design: The 7 Foundational Principles, https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf*

8 Vodafone, "Customer Privacy," *https://www.vodafone.com/content/dam/vodafone-images/sustainability/drf/pdf/vodafone_drf_customer_privacy.pdf*

9 General Data Protection Regulation (GDPR), "Art. 40 GDPR: Codes of Conduct," Intersoft Consulting, *https://gdpr-info.eu/art-40-gdpr/*

10 Ethics & Compliance Initiative, "Why Have a Code of Conduct," *https://www.ethics.org/resources/free-toolkit/code-of-conduct/*

11 Data Management Association International, "Body of Knowledge," 2017, *https://dama.org/content/body-knowledge*