Delivering Personal Data Protection Compliance on a Global Scale

Disponible également en français
www.isaca.org/currentissue

On 4 May 2016, after four years in the making, the European Union (EU) General Data Protection Regulation (GDPR) was published in the *Official Journal of the European Union*[1] and officially set an application date.[2] While the regulation entered into force on 24 May 2016, it applies going forward beginning on 25 May 2018. The GDPR is working in conjunction with, and expanding upon, the EU Directive regarding the processing of personal data to achieve the common goals of personal data protection, crime investigation and prosecution. This partnership is unveiling sweeping updates to data protection rules of which the world has not seen the likes in more than 20 years.

> *The vast majority of respondents (84 percent) indicated that they anticipate that the GDPR will impact their organization.*[3]

The new GDPR, put forth by the European Commission in 2012 and generally agreed upon by the European Parliament and Council in December of that same year, is set to replace Data Protection Directive 95/46/EC. Over the past four years, proactive companies have implemented the necessary privacy processes and procedures that comply with Directive 95/46/EC. Companies will need to do the same once again for the new protections for EU data subjects when the GDPR begins to be enforced. Substantial fines and penalties will be imposed on companies with noncompliant data controllers and processors.

The impact of this new regulation is completely pervasive. Companies with more than 250 employees that process personal data of EU citizens will be subject to the GDPR. Not only that, but GDPR applies to all private sector personal data processing by organizations of the EU and organizations outside the EU that target EU residents. Wherever such organizations transfer personal data to the EU, the GDPR's impact will be felt. Rest assured, the export regime will make sure of that. Companies meeting these definitions will be forced to comply or abandon any opportunity to engage with the significant audience of EU customers. Stiff penalties for noncompliance include fines greater than €20 million, or approximately US $23 million, and 4 percent of the company's global revenue.

Although companies of all sizes will be challenged, the GDPR most significantly impacts global companies with a broad international presence. These challenges arise from companies having to expand the scope of already very complex IT landscapes and from the cross-border transmission of personal data.

Turning Cost Into Value

Usually, any compliance is perceived as a cost. Effective companies and their leaders successfully generate value for businesses and their customers by designing and deploying responsive data privacy and compliance programs.

For example, the leading global energy management and automation provider proposed three major objectives for its worldwide personal data protection compliance initiative:

1. Put the US $1.2 billion risk of breaching personal data protection regulations[4] under control in the EU and other countries where the company operates.

Do you have something to say about this article?
Visit the *Journal* pages of the ISACA® web site *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

Ilya Kabanov, Ph.D.
Is an information technology expert with 15 years of experience in enterprise IT. He has held leading transformation roles in IT strategy, technology project management, security and data privacy in companies ranging from a successful start-up to a global US $36 billion enterprise. Currently, Kabanov provides leadership to a global applications security and personal data privacy compliance initiative for a top global energy management and automation provider. In 2013, *Kommersant Magazine* recognized him as Russia's best chief information officer in the logistics and transportation industry. Kabanov is a member of the Institute of Electrical and Electronics Engineers and the International Association of Privacy Professionals and serves as a judge at the MIT Sloan CIO Symposium.

2. Enable and support the growth of revenue and a rich customer experience in the area of mobile solutions and connected Internet of Things (IoT) solutions the company offers:

How leaders generate value through compliance:
- Expand customer satisfaction and build trustful relationships with clients
- Enable revenue growth
- Lower the cost of compliance

3. Achieve a reduction in the cost of compliance with personal data protection legislation. One way to do this is by utilizing binding corporate rules through the application of different compliance methods, including self-certification, with respect to the risk profile of IT applications and systems involved in personal data processing.

In addition, the company believes its global responsibility goes beyond regulatory compliance. The company has solid principles of conducting business ethically, sustainably and responsibly around the globe. Responsibility is the key objective at the heart of the company's corporate governance. This determines the commitment of the company to set and meet the highest standards in ethics and privacy, and enables it to shape the future of the industry by introducing tomorrow's best practices today.

"Every company's goal is compliance, but also to seek it in such a way that sustains growth and profitability."

Every company's goal is compliance, but also to seek it in such a way that sustains growth and profitability. This is not an easy task, as each company will face multiple challenges in an attempt to reach compliance.

Challenges

The GDPR and national personal data protection regulations push the need for organizations to develop and deploy risk and compliance frameworks that span numerous internal departments, including legal, security and IT, all while staying in accordance with differing legislations across multiple jurisdictions around the world. While there are different views on the processes that global organizations can adopt to establish and manage regulatory and compliance risk factors, the challenges that enterprises need to consider are actually very common. They are:

- **Complexity**—The volume and increasing complexity of the personal data protection regulatory landscape have gained momentum, particularly in the EU, the United States and some emerging countries. Global companies need to comply with a variety of regulatory legislation on national levels and ensure compliance across all business dimensions such as countries, data types and volumes, and various residencies of data processors.
- **Agility and consistency**—Agility is a necessary factor. Laws and regulations change constantly, and the time it takes for new IT products to reach the market is shrinking. Compliance with these changes must also reflect a condensed time frame to be effective. Companies must bring consistency to their compliance structures. It needs to be in real time and accurately reflect changes in rules and new regulations. Each company needs to develop and be aligned with rapid delivery cycles of IT systems and products. Compliance with new regulations means making sure that multiple systems and multiple processes are compliant, not only at implementation, but throughout the structure's life cycle.
- **Experts' capacity and availability**—The lack of IT security expertise and the scarcity of experts in the personal data protection field slow down and complicate the process of building compliance frameworks. Global companies fight for the limited number of experts who can lead complex data protection compliance programs and often experience challenges in educating employees about personal data protection.

Although companies face daunting challenges such as scale, geographic diversity, competing priorities and communications, the outlook for these companies is not all bleak. There are certain factors that will help forge a compliance framework with a great chance for success.

Real-life Frameworks

One of the examples of successful compliance frameworks was demonstrated by a global company that introduced the certification framework to ensure the security and compliance of IT applications and systems, thus guaranteeing clients, customers and employees the adequate protection of their personal and corporate data, entitlement to rights granted by legislation, and compliance with corporate and industrial standards and policies. The framework was designed to cover more than 1,000 software applications released annually, which store billions of records of structured and unstructured data and are accessed by millions of people worldwide.

At an early stage of framework development, it was recognized that the compliance process should comprehensively cover the application's journey along the whole life cycle from idea to retirement and ensure the privacy-by-design concept and data protection at every stage. The framework is based on a four-step process including risk assessment, risk mitigation, certification and post-certification audit phases (**figure 1**).

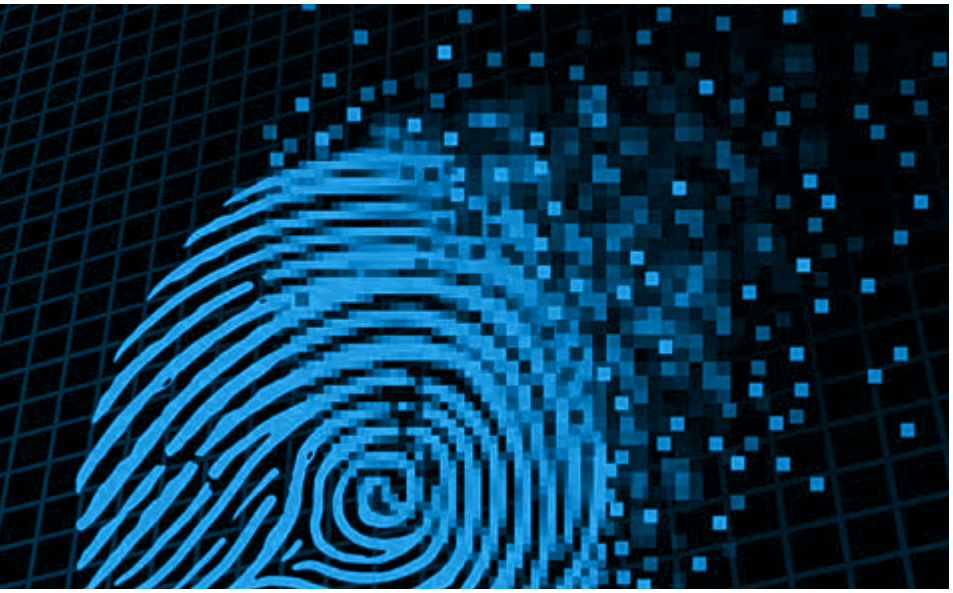
> *Once we estimated that we needed to educate 2,500 key stakeholders on a process change to achieve a high level of awareness, we collaborated with our internal communication department to design and run a yearlong multi-channel communication campaign. We leveraged internal social media, webinars, and e-learning to drive the framework's adoption, data privacy, and security risk awareness culture globally. Our goal was not only to embed the framework we designed into existing processes, but ensure that compliance becomes a part of the professional knowledge of project managers, and application delivery and operations teams.*
>
> – Enterprise Architecture Director

There are four main challenges in driving the framework design adoption:

1. The complexity of the external and internal regulatory environments. The framework had taken more than 200 laws, policies, standards and guidelines into account and then simplified them into applicable risk assessment procedures, recommendations and controls.
2. The initial maturity of policies required intensive involvement of experts for assessing risk, guiding project delivery teams on implementation and applying controls. This was a serious

Figure 1—The Phases of Ensuring Data Protection in the Project Delivery Life Cycle

Source: I. Kabanov. Reprinted with permission.



impediment for scaling the framework, therefore, the team tackled the challenge by applying an experimentation approach. This enabled the team to develop best practices and document them in the forms of hands-on guidelines for project delivery teams and application owners.

3. The complexity of an existing IT landscape where the data are processed became an additional challenge. Because of this hurdle, the team put a lot of effort into learning about the existing architecture and mapping data.
4. The large scale of the program's implementation, diverse geography of deployment and the inconsistent level of awareness about data privacy among 2,500 key stakeholders spread across all 24 time zones created a significant challenge for the rapid deployment of the framework.

The framework was the result of perfectly orchestrated and consolidated work of team members from all continents representing key functional verticals. The team has worked tirelessly across cultures, languages and time zones, all while staying focused on designing and deploying this framework.

Factor of Success

Design and deployment of compliance programs vary greatly. Each organization needs to ensure that compliance is properly embedded into current organizational processes. The more complex the organization, the more difficult it will be to ensure that privacy programs or initiatives are integrated into, or throughout, the organization.

The highest level of integration of a compliance framework into existing project and program management processes guarantees the robustness and comprehensiveness of its free-of-redundancy controls. As an example, the framework needs to be aligned with processes that may have different names in organizations, such as end-to-end project excellence and software development life cycle governance. This will help make sure that applications processing data follow the framework to ensure security and compliance at every stage of the life cycle, along with executing privacy-by-design and security-by-design principles.

Communication is a critical part of successful integration of the framework into a company's operations and projects delivery routine. Communication at the large scale of the project is a challenging exercise. To achieve success, teams need to partner with a variety of stakeholders, then design and drive a multiwave communication campaign as part of a change management process to raise awareness about the framework and educate project delivery teams on key data privacy and security risk.

Communication supports collaboration, which a recent International Association of Privacy Professionals (IAPP) survey of 550 privacy, IT and information security professionals indicated as critical in addressing data breaches. Indeed, 90 percent of those surveyed considered collaboration among the privacy, security and IT departments, together with a strong data breach response team, as most important for mitigating the risk of a data breach.[5]

Compliance to personal data privacy issues is not solely the purview of IT departments. All facets of an organization must be committed to implementing any new rules and regulations and integrating those new factors throughout every department and at every organizational echelon of the company.

Beyond Compliance

Company leaders demonstrate ethical leadership in their industries and use ethical conduct as a profit driver and competitive differentiator. A compliance framework can serve as a key component of the global cyber security and compliance portfolio of initiatives. It aims to enable and support revenue growth and provide flawless, safe and secure customer and employee experiences. While customers ask for improved productivity, precision and efficiency, companies should answer those needs through trustworthy relationships guaranteeing to customers and partners the highest level of data privacy, as well as confidentiality, integrity and availability of the information.

In addition, compliance frameworks can play a crucial role in reducing project and product delivery life cycles to support strategic business growth in primary market target areas of mobile solutions and connected IoT offerings.

Conclusion

Companies of all sizes are likely to find that GDPR compliance and implementation will not be easy. It will require thorough and flawless integration into each company's unique processes, which, in turn, will require emphasis on adequate communication and regulatory education. Most global companies are already looking to build strong compliance frameworks based on International Organization for Standardization (ISO) standards[6] and are waiting for publication of ISO/International Electrotechnical Commission (IEC) 29151:2015 Information technology—Security techniques—Code of practice for personally identifiable information protection[7] and ISO/IEC DIS 29134:2016 Information technology—Security techniques—Privacy impact assessment–Guidelines.[8]

Volatility of the regulatory environment and rapid, unpredictable geopolitical changes demand that global organizations have truly robust compliance frameworks to address possible changes in the organization's compliance needs, as well as evolving external requirements. Brexit is a perfect example of how the UK leaving the EU, coupled with the GDPR, will make compliance more challenging for global firms.

Because the UK's actual exit from the EU will take place after 25 May 2018, it is important to note that EU companies will still need to comply with GDPR. All companies processing data of UK citizens at that time will be required to comply with the UK legislation.

> **"A compliance framework can serve as a key component of the global cyber security and compliance portfolio of initiatives."**

Steve Wood, interim deputy commissioner at the UK Information Commissioner's Office (ICO), says, "The ICO's role has always involved working closely with regulators in other countries, and that will continue to be the case. Having clear laws with safeguards in place is more important than ever given the growing digital economy, and we will be speaking to the British government to explain our view that reform of UK data

protection law remains necessary."[9] Essentially, this means the UK will be evolving data protection laws and demanding organizations serving UK customers to ensure compliance in addition to the GDPR. It is important to remember that personal data protection regulations are mostly designed to help organizations achieve best practices for data protection; they are actually a good set of rules to follow. Fundamentally, the majority of personal data protection compliance requirements demand privacy by design, good information management policies, and reasonable security measures, procedures and technologies to minimize possible data loss incidents. Therefore, organizations that have designed and deployed robust compliance frameworks with a reasonable granularity of controls will be able to apply them widely, while also addressing possible regulatory changes and shifting compliance needs, to safely protect personal data and enable business opportunities.

Endnotes

1 Official Journal of the European Community, *www.ojec.com/*

2 Official Journal of the European Union, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons With Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)," 4 May 2016, *http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf*

3 Baker and McKenzie, "Preparing for New Privacy Regimes: Privacy Professionals' Views on the General Data Protection Regulation and Privacy Shield," April 2016, *http://f.datasrvr.com/fr1/416/76165/IAPP_GDPR_and_Privacy_Shield_Survey_Report.pdf*

4 European Commission, "Protection of Personal Data," *http://ec.europa.eu/justice/data-protection/*

5 International Association of Privacy Professionals, "How IT and Infosec Value Privacy," *https://iapp.org/resources/article/how-it-and-infosec-value-privacy/*

6 International Organization for Standardization, ISO/IEC 27018:2014 *Information technology—Security techniques—Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*, 1 August 2014, *www.iso.org/iso/catalogue_detail.htm?csnumber=61498*

7 International Organization for Standardization, ISO/IEC DIS 29151 Information technology—Security techniques—Code of practice for personally identifiable information protection, 5 July 2016, *www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=62726*

8 International Organization for Standardization, ISO/IEC DIS 29134 *Information technology—Security techniques—Privacy impact assessment—Guidelines*, 18 July 2016, *www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=62289*

9 Wood, S.; "GDPR Still Relevant for the UK," Information Commissioner's Office, 7 July 2016, *https://iconewsblog.wordpress.com/2016/07/07/gdpr-still-relevant-for-the-uk/*