FEATURE

Data Privacy, Data Protection and the Importance of Integration for GDPR Compliance

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/2QKJNBq

日本語版も入手可能
www.isaca.org/currentissue

The EU General Data Protection Regulation (GDPR) guidelines require that organizations protect the personal data and privacy of EU citizens not only for transactions that occur within the European Union, but also any transaction affecting EU citizens, regardless of their location. It is a colossal order, since all organizations—regardless of their location—that control or process personal data of subjects in the European Union must comply with GDPR.

And what exactly do personal data entail? According to GDPR, personal data span any information "relating to an identified or identifiable natural person ('data subject')"[1] and such identifiers can include a name, some sort of identification number, an email address, or even "one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."[2]

There are essentially two main responsibilities for organizations to meet GDPR compliance: They must store and manage personal data in a way that makes the data accessible and removable for the data subject, and they must secure and protect those personal data in transit and at rest. But those responsibilities change whether the organization is the data processor or data controller, though many organizations act as both in some capacity.

A processor is a "natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller."[3] The controller refers to the "natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of processing of personal data."[4] Simply put, controllers collect the data and processors do something with the data. But both controller and processor must act in compliance with GDPR and protect data from unauthorized access, destruction, loss and disclosure.

> "DATA PRIVACY AND DATA PROTECTION CERTAINLY ARE SIMILAR TERMS AND OFTEN OVERLAP, BUT THEY ARE NOT ALWAYS SYNONYMOUS."

It is important to dive deeper into the nuances of the terms "privacy" and "protection" as they relate to digital data movement and data processing, as such nuances can have different implications in how enterprises manage personal data and meet GDPR compliance mandates.

Privacy and Protection

Data privacy and data protection certainly are similar terms and often overlap, but they are not always synonymous. Data protection is the practice or process of safeguarding information from corruption and loss. Data privacy (or information privacy) is related to organizations' processing rules and practices and regulates controllers and processors from using data in a wrongful manner.

Dave Brunswick
Has more than 25 years of experience in technical sales, presales, technology strategy, engineering, product management and product development, including holding senior consulting and architecture roles throughout the managed file transfer software market. He currently serves as vice president of North America presales and solution support for Cleo.

More simply, data protection involves securing data against unauthorized access, while data privacy involves what happens with those who have authorized access. Data protection is usually centered on securing information and may include encryption, secure communications protocols and measurable security policies. Data privacy might best be considered a legal issue that focuses on how personally identifiable information (PII) is collected, stored and used. The focus of data protection, then, is security, whereas data privacy has more to do with how the information is governed and used.

Such differences are important to the privacy and cybersecurity discussions facing organizations today, especially those subject to compliance mandates such as the US Sarbanes-Oxley Act (SOX), the US Health Insurance Portability and Accountability Act (HIPAA), and, of course, GDPR. Consequently, both the movement and processing of data—and the business procedures around those workflows—must be considered, measured and monitored to adhere to required compliance standards.

In a digital business context, data protection does not always equal data privacy, and, although it is possible, it is extremely difficult to ensure privacy when digital data are not protected by technology. If someone can maliciously use an individual's personal information, its privacy is wholly uncertain. It is important that organizations that act as the data processor and controller employ data protection technologies, including copy data protection, encryption, managed file transfer (MFT), secure integration and others that help to fortify the governance processes of the data.

The Importance of Processes

The GDPR mandate puts considerable emphasis on data processes, including the integration and ingestion—the processing—of the data. Thus, organizations are beginning to think about privacy from not only a protection standpoint (how they can secure it anywhere), but also from a process protection standpoint (how they can govern data use every step of the way).

Because nearly everything an organization does with data constitutes processing; virtually every process involves data transfer at some level. For industries including healthcare, financial services, and logistics and transportation, data transfer is core to basic operations, and any action on data,

including internal transfers, external transfers, storage, viewing, analyzing, changing, synchronizing and replicating, is, technically, a processing event.

Examining the broader chain of custody around these events in correlation with every interaction and every process outlined by GDPR, data transfer is there. In fact, organizations may find it useful to ask themselves some questions about their overall technology stack:

- How do business-to-business (B2B) data move through the enterprise resource planning (ERP) software, electronic data interchange (EDI) systems, and transportation and warehouse management systems along the supply chain?
- Does the organization transform a partner's flat file into an IDOC so it can ingest into the organization's SAP system?
- If the organization uses a cloud storage repository, what is the cloud integration process that gets the data there safely?
- For the Salesforce customer relationship management (CRM) system powering the organization, what integration processes have to happen to keep it up to date with purchasing, billing and shipping information from other applications?
- How is information moved into and out of the data warehouse feeding the data analytics platform?

Even though it is behind the scenes for most organizations, data movement is at the core of every business process, and it is an organizational responsibility to protect that data in all manner of transfer, including B2B, ground to cloud, system to

> IF ANY ACTION ON DIGITAL DATA THROUGHOUT THE ECOSYSTEM IS TECHNICALLY A PROCESSING EVENT, TECHNOLOGY MUST BE IN PLACE TO PROPERLY SECURE AND GOVERN THOSE EVENTS.

system, application to application, system to person, and person to person.

If any action on digital data throughout the ecosystem is technically a processing event, technology must be in place to properly secure and govern those events. So how do these organizations, which are simultaneously data processors and controllers, employ the right balance of technology usability, security and governance to ensure that data get moved, integrated and processed in accordance with their compliance needs? The answer for many organizations is ecosystem-driven integration platforms.

Safeguarding Data and Data Processes

In the new world order of GDPR and the associated need to secure and govern data flows across firewalls, the road to compliance is paved with technology. GDPR and other compliance mandates require organizations to provide some level of personal data protection and, to do that, organizations need to secure, govern and control their data flows and prevent unauthorized access and use.

Encryption and secure file transfer technology are common means of protecting data, but they do not explicitly enable the data's privacy. The governance and policy enforcement mechanisms do that. So, for many purposes, data privacy is a subset of data protection and is often a side effect of smart policy when that policy provides broader protection.

In a B2B landscape, business data move among systems, applications and people that organizations cannot inherently control. That is why compliance and governance—key aspects of the modern business ecosystem—are so difficult to implement without the right core integration platform. Modern organizations gain a step in providing both protection and privacy of digital personal data when they upgrade their data processes using advanced integration technology.

Ecosystem-driven integration platforms protect data processing events when data are in transit and at rest with end-to-end encryption so that only authorized users can access the data. They also provide mechanisms to govern and control every aspect of the integration process, whether application programming interface- (API-) or file-based integrations. This governance, enabled by a robust orchestration engine and Representational State Transfer (RESTful) APIs supporting automation, consistency and dependability, ensures that personal and sensitive information can be properly handled, whether encrypted or not. **Figure 1** shows a traditional model, and **figure 2** shows an ecosystem-driven integration platform.

Protection of those interactions and the processes surrounding them is just as critical. It requires support for a multitude of methodologies and standards, including standards for securing and managing all aspects of data movement, and securing the platform and providing robust auditing and reporting around access, initiation and termination of any integration-dependent process.

Conclusions

The cost of GDPR noncompliance can have dramatic implications. Organizations may be penalized up to 4 percent of their annual turnover for a data breach or data misuse, not to mention the damages to the organization's brand, reputation and credibility.

GDPR forces organizations to evaluate, test and update how data are collected, moved and processed, for the goal of protection and, ultimately, privacy. Organizations are now required to publish clearly stated privacy policies that help individuals understand the digital information collected and

Figure 1—Traditional Model

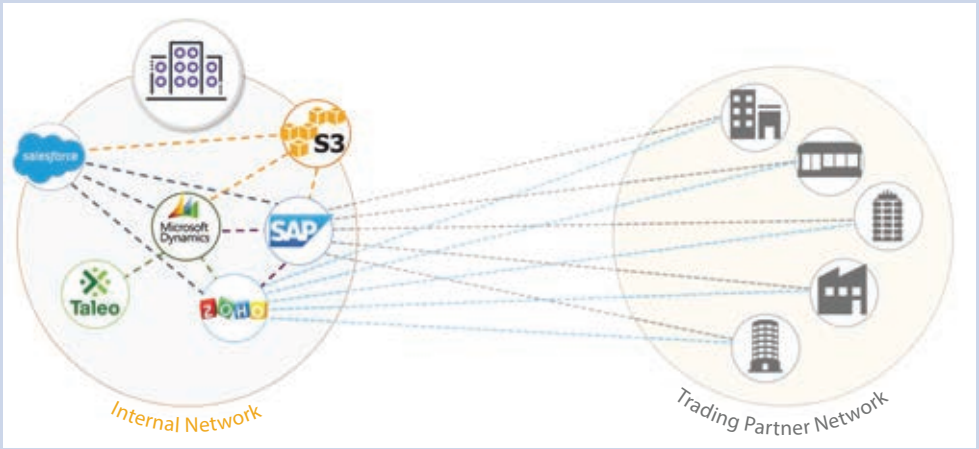

Figure 2—Ecosystem-Driven Integration Platform

why it is collected. Many organizations, including Google and Facebook, even detail how a user can manage and delete that information.

This means organizations around the world, mandated to improve how they collect, store and use personal data, are evaluating, testing and adopting modern ecosystem-driven integration technology to safeguard data and employ the governance processes that ensure privacy and compliance.

While data protection may not inherently guarantee data privacy, there is little way to deliver on the promise of privacy without it. But with the tools to secure the data and the procedures to reliably govern the data's use, the right integration platform gives the organization the ability to do both.

> "WHILE DATA PROTECTION MAY NOT INHERENTLY GUARANTEE DATA PRIVACY, THERE IS LITTLE WAY TO DELIVER ON THE PROMISE OF PRIVACY WITHOUT IT."

Endnotes

1 GDPREU.org, "Personal Data," *https://www.gdpreu.org/the-regulation/key-concepts/personal-data/*
2 *Ibid*.
3 GDPREU.org, "Data Controllers and Processors," *https://www.gdpreu.org/the-regulation/key-concepts/data-controllers-and-processors/*
4 *Ibid*.

Enjoying this article?

- Learn more about, discuss and collaborate on information security management ISACA's Online Forums. *https://engage.isaca.org/onlineforums*