Seven Key Concepts Organizations are Getting Wrong About the Global Privacy Law

By Barclay T. Blair

On May 25, 2018, the European Union's (EU's) General Data Protection Regulation[1] (GDPR)—hailed as "the most important data privacy regulation in 20 years"—took effect.[2] Most people who are familiar with the GDPR have also heard about the huge financial penalties that face those who don't comply with the law—totaling up to either nearly $25 million or four percent of an organization's annual global revenue. Yet, there remains a great deal of confusion and uncertainty about the real impact of the GDPR.

In the absence of real knowledge, the Information Governance Initiative's (IGI) research and discussions with information governance (IG) professionals have revealed that "tall tales" and "urban myths" are being shared about the regulation, particularly about the impact it is likely to have on organizations that operate outside the EU. Although it is impossible to definitively answer some questions about the GDPR until authorities begin enforcing the law, there is less uncertainty about its most important provisions and what organizations must do to prepare and comply.

IGI, which has identified some of the most common misconceptions, recently released a white paper to put some of these GDPR myths to bed.

Myth #1: GDPR Only Affects EU Companies

The EU states that GDPR is specifically and unambiguously intended to extend EU data privacy law outside of the EU. The intention is "to ensure that natural persons are not deprived of the protection" of the GDPR even when their data is processed by non-EU companies, or outside of the EU.

GDPR applies to organizations based in the EU that process personal data either inside or outside the EU. In addition, the GDPR applies to organizations outside the EU that process the personal data of EU citizens related to offering goods or services (whether paid or free), or the monitoring of behavior when that behavior takes place in the EU. Monitoring includes tracking EU citizens "on the internet," especially where the monitoring data is used to "profile" a person based on their browsing habits, location, or other information.

Reality #1: The rules follow the data.

Myth #2: GDPR Only Applies to a Limited Set of Data that is Obviously Personal

Article 4 of the GDPR expands the definition of "personal data" and thus the types of information that are regulated. While the GDPR targets more familiar forms of personal data (i.e., national ID numbers, date of birth, address, etc.) it expands its definition to include less familiar types, including "location data" and "an online identifier to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person" (GDPR Article 4).

It also restricts the processing of many forms of personal data including data "revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership," and various forms of health data. However, these restrictions are not absolute. They do not apply if one of 10 GDPR provisions exists including, for example, that such processing is necessary for an employer to provide benefits programs (GDPR Article 9).

Reality #2: More data than ever is considered "personal" by GDPR, creating more complexity and cost.

Myth #3: The GDPR Data Breach Notification Requirement is Straightforward

US organizations should not assume that their current data breach notification programs are sufficient to satisfy GDPR obligations. Under the GDPR, organizations have an obligation to protect personal data. GDPR considers a "breach" to include more than just theft or exposure of private data. It also includes "accidental or unlawful destruction, loss, or alteration" of data, for example.

Many practitioners may be aware of a "72 hour" clock for notifying supervisory authorities about a data breach under GDPR, but not all understand that the clock for notification begins ticking once an organization becomes aware of the breach, not after the breach has occurred. Notification of supervisory authority in the jurisdiction(s) where the data breach occurred must be done in all cases where the breach represents a "likely risk" to the affected individuals.

Reality #3: Data breach notification requires many complex decisions to be made quickly.

Myth #4: Individuals in the EU Must Always be Notified of a Data Breach

Notice to individuals is subject to a higher threshold than notice to authorities. An organization may have to directly notify affected individuals as well as the relevant regulatory authorities when there is a "high risk" to the rights and freedoms of the affected individuals due to a breach (GDPR Article 34(1)).

Practitioners should be aware that there are certain instances where notification to individuals is not required:

- When breached personal data is encrypted
- When immediate action was taken to eliminate the risk post-breach
- When notification would require "disproportionate effort"; for example, if the organization does not have means of directly contacting the individuals affected

However, under Article 32, a supervisory authority has the power to require individual notification, even if the organization has concluded that the data breach did not reach the "high risk" threshold.

Reality #4: Notification of individuals is not always required.

Myth #5: The Consequences of GDPR Failure are

Potentially Large, But Contained

If an IG practitioner only knows one thing about the GDPR, most likely it is that their organization can face administrative fines of up to $25 million or four percent of annual global revenue, whichever is greater. These eye-popping fines are intended to be "effective, proportionate and dissuasive," according to the GDPR's Article 83.

Yet the GDPR also makes it clear in GDPR Recital 150 that "[i]mposing an administrative fine or giving a warning does not affect the application of other powers of the supervisory authorities or of other penalties." Supervisory authorities have the power to impose both administrative fines and corrective measures. These corrective measures could have a much more profound effect for those organizations that process personal data as a core revenue-generating activity than even the maximum administrative fine.

Reality #5: The consequences of failure are not limited to EU administrative fines. Organizations may also face sanctions, lawsuits, corrective actions, and other consequences.

Myth #6: Only Brand New GDPR Privacy Right is 'The Right to be Forgotten'

The very first provision of the GDPR states that privacy is a "fundamental right." To this end, the GDPR enshrines several privacy rights, including:

- Right of access, as found in Article 15
- Right of rectification, as found in Article 16
- Right to erasure (right to be forgotten), as found in Article 17
- Right to restriction of processing, as found in Articles 18 and 19

- Right to data portability, as found in Article 20
- Right to object, as found in Article 21
- Right to not be subject to automated decision-making and profiling, as found in Article 22
- Right to be informed, as found in Articles 13 and 14

Additionally, Article 12 states that organizations must be prepared to act on requests from data subjects "without undue delay, and in any event within one month of the request."

Reality #6: The GDPR enshrines several privacy rights that might not be addressed by many existing privacy programs.

Myth #7: The GDPR's Privacy Rights Apply to All Sensitive Information

Log files generated by servers, firewalls, and a range of additional enterprise technologies often contain sensitive information about an individual's interaction with those systems. But, at this stage, it is unclear whether these kinds of technical log files meet the GDPR's definition of "personal data" and, as such, whether they are subject to all its requirements.

Useful guidance regarding security and system log files can be found in the GDPR's exception (discussed in more detail in IGI's full white paper on this subject).[3] However, the ultimate answer to this question will depend on how the GDPR is enforced and interpreted by the courts.

Reality #7: Log files and other kinds of sensitive information may not be subject to the GDPR's access, storage limitation, or other privacy rights.

GDPR Creates Greater Need to Control Data

Taken as a whole, the impact of GDPR will be felt in the new level of profound insight and control that organizations must have over their data.

Although GDPR is a very significant regulation, it stands only as the latest example of the myriad ways that the collection, use, storage, and governance of information is being regulated. Whether the focus of this regulation is privacy—as is the case with GDPR—or cybersecurity, financial transparency, or recordkeeping, these laws and regulations share a singular theme: organizations need to understand and govern their data.

While myths and misconceptions may abound, one thing is certain—organizations with well-built and mature IG programs are best positioned to adapt to the requirements of GDPR.

Notes

1. European Union General Data Protection Regulation. https://gdpr-info.eu/.
2. Trunomi. European Union General Data Protection Regulation education webpage. www.eugdpr.org.
3. Information Governance Initiative. "GDPR Myths and Misconceptions." https://iginitiative.com/download-igis-whitepaper-gdpr-myths-misconceptions/.

Barclay T. Blair (Barclay.blair@iginitiative.com) is the founder and executive director of the Information Governance Initiative.

Article citation:
Blair, Barclay T. "Seven Key Concepts Organizations are Getting Wrong About the Global Privacy Law ." *Journal of AHIMA* 89, no.6 (June 2018): 44-45.