With its sweeping scope, demanding requirements and significant enforcement fines, the European Union (EU) General Data Protection Regulation (GDPR) is not quite like any other privacy regulation—which can make compliance with it seem quite a daunting proposition. But it’s important to remember that even though many aspects of the regulation are unprecedented, GDPR didn’t come out of nowhere. An understanding of the regulatory environment from which it emerged and the rules from which it evolved can help organizations as they consider how to meet its requirements now, and as they look ahead, what it will require of them in the future. In the spirit of helping achieve that understanding, this paper:

- Presents highlights of the recent history of privacy laws and illustrates how organizations can build on prior strategies for compliance as they work toward GDPR compliance
- Summarizes some of the main provisions of the regulation today, including who is affected, requirements for compliance and penalties for failing to comply
- Explores the continuing evolution of GDPR, including implications for doing business going forward within the context of the regulation

Foundation for action: Privacy regulation’s past

The principle is simple: The more work an organization has done to comply with applicable privacy laws and regulations over the years, the better prepared it should be to comply with GDPR.

Mature organizations that have created effective privacy programs as part of their efforts to meet the requirements of existing rules may well find that GDPR compliance is much less of a heavy lift than it would be without that data protection foundation. By looking back at the recent history of privacy laws, organizations can assess the work they’ve already done to address existing requirements, with an eye to building on it to address GDPR data protection compliance.

The following isn’t intended to be a comprehensive history of privacy laws, but a set of highlights intended to provide some historical context for GDPR, as well as to help organizations think about how their current compliance posture around privacy laws may serve as a basis for GDPR compliance.
The EU Data Protection Directive, which was adopted in 1995 to protect the privacy of the personal data of EU citizens, rests on many of the same tenets as GDPR—including the belief that people whose data is collected should be informed of it and should be allowed access to personal data collected about them. GDPR builds upon the existing directive by establishing a single set of rules that applies to EU Member States.

GDPR protects data based on the location of data subjects, rather than on the location of organizations that collect data, which makes it applicable to organizations in non-EU countries. GDPR also imposes a high cost for noncompliance in the form of stiff financial penalties that can climb to hundreds of millions of euros, depending on the organization’s annual revenue.

Compliance now: GDPR in brief

Here’s a quick look at the present state of GDPR: who and what the regulation covers; specific requirements focusing on new rules, such as the much-discussed “right to be forgotten” and the 72-hour breach notification requirement; and penalties for not complying.

Scope

Under the GDPR, companies processing personal data must continue to ensure for these processing activities that they have proper controls on how personal data is stored, kept up to date, accessed, transferred and deleted, and that they have implemented appropriate technical and organizational security measures.

As to what the regulation covers, "personal data" is widely defined to mean any information relating to an identified or identifiable individual (known as a "data subject" under GDPR). Personal data may include name, physical address, email address, identification number, location data, online identifier, credit card number, economic/cultural/social identity or health information (i.e., genetic, mental, physical and physiological data).

GDPR requirements

GDPR contains a number of requirements for protecting the privacy of personal data. There are far too many to list and explain in this paper, but you can refer to the regulation itself for more information. The requirements are also well summarized in A Practical Guide for GDPR Compliance, an Osterman Research white paper sponsored by RSA and eight other leading technology companies. For our purposes here, let it suffice to describe a few of the regulation’s new requirements that increase data subjects’ access to and control over their personal data—requirements that some data controllers and processors may already have a head start on meeting.

• The right to access allows data subjects to obtain a copy of their personal data from a data controller.
The right to data portability means the right to transfer their data to themselves or to another controller if they so desire. Organizations that are already using GRC solutions to identify and catalog business processes or applications associated with personal data for other compliance purposes have a foundation to more readily support this requirement.

The “right to be forgotten” entitles data subjects to request that an organization that controls their personal data erase the data, stop disseminating it and have third parties stop processing it. GRC solutions that an organization is already using to understand business processes associated with personal data for other compliance purposes may prove useful in meeting this requirement. They may facilitate the implementation of processes to respond in a timely manner to these requests.

Breach notification, or the right to know when one’s personal data has been breached, is not a new concept in privacy law, but not all breach notification rules have a tight timeline attached to them the way GDPR’s rule does. Organizations that have technology in place to detect threats and data breaches may find such solutions useful in their efforts to comply with GDPR requirements to inform regulators and data subjects of a breach, assuming the technology supports a strategy of rapid detection and response.

The “organizational and technical” protection referred to in GDPR requires several integrated components to work. Organizations not only need to understand their data processing activities but also carry through with risk and compliance processes that implement appropriate controls based on risk. Common concepts in data protection, such as policies and standards, identity management, access control, data governance, system monitoring and encryption, are clearly applicable and must be part of the strategy.

Penalties

Enforcement of GDPR data protection rules begins May 25, 2018, after which organizations in violation of the requirements may be subject to sanctions such as warnings, suspension of data transfer, ban on processing activities and severe financial penalties. There are two tiers of penalties, as described in Article 83 of the regulation:

- Two percent of revenue or up to 10 million euros (whichever is higher) for infringement of provisions relating to the obligations of the data controller and processor, the certification body and the monitoring body
- Four percent of revenue or up to 20 million euros (whichever is higher) for infringements of provisions relating to the basic principles for processing, including conditions for consent; the data subjects’ rights as spelled out in the regulation; international transfers of personal data; and non-compliance with the supervisory authority’s orders

“Whichever is higher” is an important point here. For example, 20 million euros may sound like a lot, but keep in mind that a global company with revenues of 5 billion euros could be looking at ten times that much.
Ongoing compliance: Evolving with GDPR

As the May 25 deadline approaches, it's easy to think of compliance as the culmination of a long effort to meet the many requirements of a major new privacy regulation. But there's also an argument to be made for thinking of GDPR not as an ending point, but as a starting point. As Keith Enright, Google’s Legal Director, Privacy, has cautioned, one of the “greatest dangers” associated with GDPR compliance is “tacking toward 2018 and thinking you’re done.” Compliance is much more likely to be an ongoing effort that will evolve as the law evolves.

No matter how GDPR evolves, though, one thing is certain: Organizations with a firm foundation in privacy risk management and data-governance frameworks will be in the best position to pivot and adapt to changes in the regulation. The work they’ve already put in to comply with privacy compliance requirements will continue to serve them well, and the additional efforts they undertake to comply with GDPR will benefit them going forward as the law continues to evolve.

Learn about RSA solutions to help with GDPR compliance at rsa.com/gdpr

About RSA

RSA, a leader in cybersecurity and risk management solutions, provides organizations with technology to address challenges across security, risk management and fraud prevention in the digital era. RSA solutions are designed to effectively detect and respond to advanced attacks; manage user access control; and reduce operational risk, fraud and cybercrime. RSA protects millions of users around the world and helps more than 90 percent of the Fortune 500 companies thrive and continuously adapt to transformational change.
For more information, go to rsa.com.