The New EU General Data Protection Regulation—Benefits and First Steps to Meeting Compliance

The European Data Protection Directive (Directive 95/46/EC) was published on 13 December 1995, and fully implemented by 24 October 1998.[1] At that time, email applications were not ubiquitous; Facebook, Twitter and LinkedIn did not exist; and e-commerce was still in its infancy, but already showing great potential for expansion. During the next 20 years, technology transformed the world into an interconnected society that trades in information. New communication and interconnection capabilities call for new data protection rules. Therefore, the European Union (EU) issued the General Data Protection Regulation (GDPR) on 14 April 2016 to supersede Directive 95/46/EC. The new regulation is expected to be fully implemented by 25 May 2018.[2]

The EU groups the expected benefits from the GDRP into three categories:

- Better protection for personal data
- More opportunities for business
- More consistent application and effective enforcement of the rules

Eva Sweet, CISA, CISM
Is the director of integrated audit guidance at the Institute of Internal Auditors and an IT professional with more than 15 years of experience in IT operations, security and audit. Most recently, she was a technical research manager at ISACA® where she authored thought leadership and practical guidance publications that focused on risk and assurance, including this article.

What are the benefits and impacts of the GDRP on enterprises that are in the EU and those that are outside of the EU and doing business with EU nations? What are the first steps towards meeting GDPR compliance?

Better Protection for Personal Data

The EU GDPR clearly defines the rights of the individual and the obligations of entities that are processing or responsible for the processing of data. However, the most important aspects of this new regulation are the enactment of compliance assessment mechanisms, sanctions for noncompliance and a single framework that must be adopted by all EU members consistently.

Many of the enhancements to data protection in the EU are directly related to concerns expressed by EU citizens. In March 2015, the Directorate-General for Justice and Consumers conducted a survey that asked 28,000 EU citizens about their impression of data protection programs in the EU. The Eurobarometer 431[3] survey results show that:

- A large portion of the respondents (71 percent) understand that providing personal data as part of everyday transactions will be the norm.
- The top three concerns related to personal data are:
  - Becoming a victim of fraud (50 percent)
  - Having one's online identity used for fraudulent purposes (40 percent)
  - Having one's information used without one's knowledge (32 percent)
- 62 percent of respondents said that they do not trust their Internet service providers (ISPs) and 63 percent said that they do not trust online businesses to protect their data.

The results of the survey were not a surprise for the EU Council; in fact, the results were confirmation that enhancements to data protection will address concerns currently shared by most EU citizens. Some of the improvements to data protection to offer better protection to personal data include:

- Ensuring that consent to process data is granted by means of a clear, affirmative action

- Disclosing more and clear information about data processing
- Guaranteeing easy access to personal data and the freedom to move data from one service provider to another (portability)
- Mandating the implementation of stricter safeguards for transfers of personal data outside the EU
- The right to be notified if data is compromised
- Limits on the use of automated processing of data to make decisions that can harm the individual
- The right to rectify and remove data including:
  – The right to be forgotten
  – The right to erase personal data

> **"Globalization, cloud computing, the Internet of Things and social networks are compelling reasons to reform data protection."**

More Opportunities for Business

The modernization of data protection is the EU answer to the rapid changes in the technology environment and the disappearance of physical boundaries around data and the infrastructure that is used to collect, process, store and transmit data. Among other factors, globalization, cloud computing, the Internet of Things (IoT) and social networks are compelling reasons to reform data protection and start providing mechanisms to protect data that are constantly moving across jurisdictions in the blink of an eye.

The implementation of GDPR across all 27 EU member countries is intended to lay the foundation for the Digital Single Market project,[4] which is an initiative to boost the digital economy by enabling European citizens and businesses to fully exploit the benefits of globalization and e-commerce. The main changes to the data protection approach to create more opportunities for business include:

- The introduction of a single set of rules that are technology neutral and futureproof across the EU[5]
- Clear rules on when EU law applies to data controllers outside the EU
- Robust provisions on data security, data protection by default and data protection by design to increase consumer confidence in the online environment
- New rules that allow small and medium-size enterprises (SMEs) to participate in the digital single market
- A risk-based approach to match controller's obligations to the level of risk in data processing
- Similar opportunities for EU and non-EU enterprises offering goods and services to EU citizens

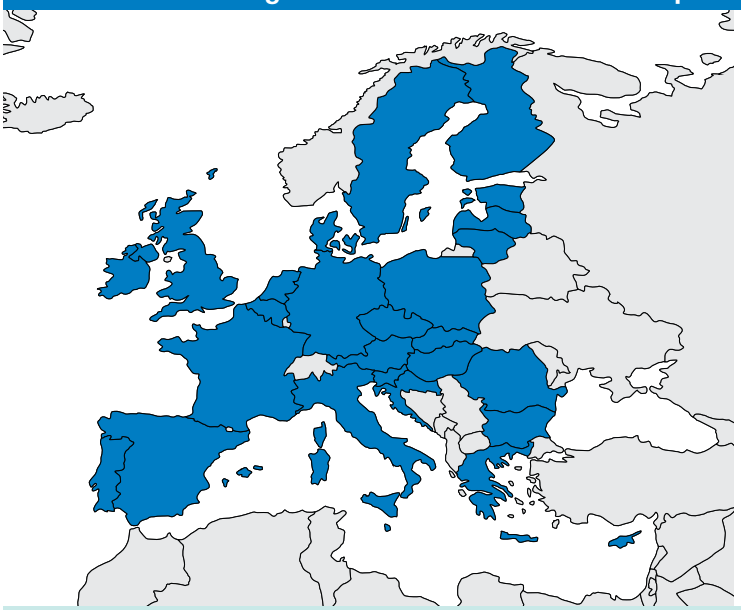
More Consistent Application and Effective Enforcement of the Rules

Data protection in the EU has been inconsistent due to the nature of Directive 95/46/EC that allows member countries freedom to tailor the directive to their perceived needs. The problem of having multiple versions of the same set of rules was not as serious 20 years ago when Directive 95/46/EC was implemented, but as the EU continues to expand (**figure 1**), the need for a common approach to data protection and compliance reporting is critical. The new EU GDPR is a significant step toward standardization and harmonization of data protection rules and obligations.

The main changes to the data protection approach to unify and standardize data protection requirements include the following:

- All member countries are required to implement GDPR the same way (customization is not allowed).

Figure 1—List of Countries and Map of the EU in 2016



Member Countries:

Austria	Italy
Belgium	Latvia
Bulgaria	Lithuania
Croatia	Luxembourg
Cyprus	Malta
Czech Republic	Netherlands
Denmark	Poland
Estonia	Portugal
Finland	Romania
France	Slovakia
Germany	Slovenia
Greece	Spain
Hungary	Sweden
Ireland	

The EU consists of 27 member countries (this figure already excludes the UK, which is in the process of separating from the EU). Six candidate countries are in the process of integrating EU legislation into national law to become members.[6] Candidate countries are: Albania, Montenegro, Serbia, The former Yugoslav Republic of Macedonia and Turkey.

Source: S. Solberg Licensed under the Creative Commons Attribution 3.0 Unported license.

- Businesses and citizens are able to contact the same data protection authority closer to their locations.
- Businesses report compliance assessment results for multiple locations to only one agency.
- Better cooperation among national data protection authorities is encouraged.
- Notification obligations for each country where the business operates are eliminated.

How the EU GDPR Impacts Enterprises

The impact on enterprises depends on their geographical locations, nature and extent of contact with EU citizens, and the maturity of their own data protection programs. The intention of the EU Commission is to provide better data protection to individuals, improve business opportunities and reduce the overhead of complex compliance reporting. For enterprises trying to penetrate the EU market, the GDPR may offer more benefits than impacts; but for enterprises that have an established presence in the EU, the impacts may, at first, seem greater than the benefits. Enterprises in EU member countries will not have a choice because the data protection rules are a statutory requirement, but enterprises outside the EU can determine if the benefits of doing business in the EU are greater than the impact that is associated with compliance readiness efforts.

The balance between benefits and impacts will be influenced by the level of investment required to implement GDPR.

Benefits

Some of the benefits of implementing GDPR include:

- The simplification of international data transfers (for EU and non-EU countries)
- The regulation being technology agnostic. Therefore, enterprises can implement cost-effective mechanisms to achieve compliance.
- Provisions to ensure long-lasting data protection solutions (protection by default and protection by design), which can improve return on investment (ROI)
- Consumer trust is expected to improve, which, in turn, should increase online trade (This benefit may be realized faster because improving data protection can improve trust and loyalty with current customers.)
- Provisions to ensure that SMEs can compete in the digital market. For example, undue administrative burdens will not be imposed on SMEs, nor will they be obligated to appoint a Data Protection Officer (DPO).
- The reduction of bureaucratic paperwork helping enterprises move funds from expenses to investments in innovation projects

Impacts

The first thing that enterprises of all sizes must understand is that GDPR is enforceable with penalties that, depending on the size of the enterprise, can be substantial (**figure 2**).

Figure 2—Penalties for Noncompliance[7]

Level 1	Fines of up to €10 million or up to 2 percent of total worldwide annual turnover (whichever is the greatest)
Level 2	Fines of up to €20,000,000 or up to 4 percent of total worldwide annual turnover (whichever is the greatest)

New GDPR compliance obligations can impact the enterprise by requiring these changes:

- Appointment of an independent, criminally liable DPO for data controllers and processors
- Improved/implemented data governance practices
- Improved/implemented vendor management practices
- Improved/implemented record management processes
- Implementation of technical and organizational measures to ensure that data can be accessed and updated by the individual, are portable and can be deleted across all instances in which they exist (including third parties)
- Provisions on data security, data protection by default, and data protection by design with the implementation of technical and organizational measures that ensure a level of security appropriate to the risk of individuals
- Safeguards integrated into the data processing technology and processes to ensure that citizen's rights are protected by design

> **"The first thing that enterprises of all sizes must understand is that GDPR is enforceable with penalties that...can be substantial."**

First Steps to Meeting GDPR Compliance

An enterprise cannot protect that which the enterprise does not know exists. The first step in any improvement process is to define the scope; in this case, the process to improve data protection is to identify all data elements (and instances) that must be protected in accordance with GDPR. This may sound simple, but, in reality, the task is daunting because the volume of data that any given enterprise can accumulate is massive and most likely fragmented and/or redundant. Nonetheless,

data must be located, classified and labeled in order to set a scope.

Using guidance from COBIT® 5's implementation and the continuous improvement life cycle approach, the steps shown in **figure 3** are recommended to start the process to establish a data protection program that will comply with the EU GDPR in 2018 when the implementation must be completed:

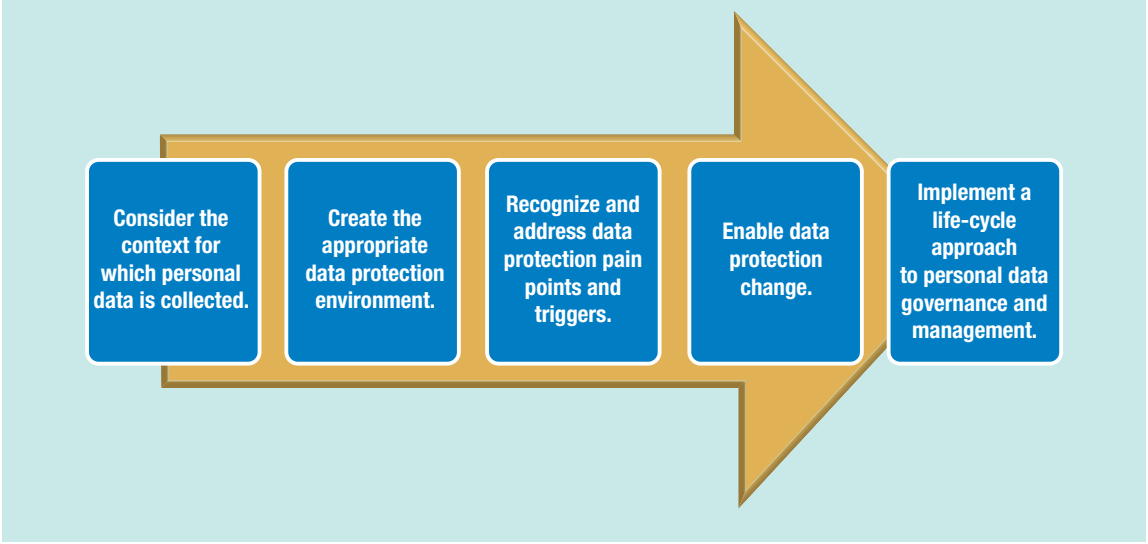
- **Consider the context for which personal data is collected,** and how it is used within the enterprise's business and privacy context—identify, classify and label data
- **Determine how to create** the appropriate data protection environment that aligns organizational needs and GDPR requirements—assess current state, identify gaps and correct issues
- **Define criteria** for recognizing and addressing data protection pain points and trigger events
- **Enable data protection change** through technical and organizational measures—embed data protection by default and by design into all business processes and technology solutions
- **Implement a life-cycle approach** to data governance and management

COBIT® 5 Implementation[8] guide provides practical and comprehensive guidance on the implementation of the continuous improvement life cycle.

Conclusion

The GDPR, unlike its predecessor Directive 95/46/EC, is an enforceable regulation that includes clear expectations for entities controlling and/or processing personal data to provide solutions that enable the protections granted to EU citizens such as the right to be forgotten, data erasure and data

Figure 3—Steps to Prepare the Enterprise's Environment for the GDPR



portability, to name only a few. Compliance with the regulation will represent a burden as enterprises must invest resources to implement and maintain the controls necessary to demonstrate compliance with the regulation. However, the GDPR mandates will also bring benefits for enterprises, especially SMEs, by improving competition in the digital market and improving the process for reporting compliance by having the same rules apply to all country members alike.

Endnotes

1 EUR-Lex, Protection of Personal Data, *http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Al14012*

2 European Union, *Official Journal of the European Union*, vol. 59, 4 May 2016, *http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=NL*

3 Jourová, V.; *Data Protection Eurobarometer Factsheet*, European Commission, June 2015, *http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_eurobarometer_240615_en.pdf*

4 European Commission, "Digital Single Market for Business and Consumers," *http://ec.europa.eu/growth/single-market/digital_en*

5 Jourová, V.; *How Will the EU's Reform Adapt Data Protection Rules to New Technological Developments?* European Commission, January 2016, *http://ec.europa.eu/justice/data-protection/document/factsheets_2016/factsheet_dp_reform_technological_developments_2016_en.pdf*

6 European Union, *"Member Countries of the EU,"* 8 April 2016, *http://europa.eu/about-eu/countries/index_en.htm*

7 *Op cit,* European Union, May 2016

8 ISACA, *COBIT® 5 Implementation*, USA, 2012, *www.isaca.org/COBIT/Pages/COBIT-5-Implementation-product-page.aspx*