Defining Data in the New Paradigm Shift: The Directive vs. General Data Protection Regulation

Elizabeth Janko
Risk Analyst
Ernst & Young
Chicago, IL, USA.

Scott A. Yetmar
Associate Professor of Accounting
Cleveland State University
Cleveland, OH, USA.

Abstract

The countless ways data is accessed and protected in Europe, with the arrival of a major European Union (EU) regulation, the General Data Protection Regulation (GDPR), will mandate modifications to company business and information technology (IT) planning with the EU as well as outside territorial business ventures. The financial services base will need to develop an effective security plan with robust breach response variations, while building an infrastructure willing and able to transform into the paradigm data transparency shift – empowered data security rights of all individuals classified as EU citizens. Personal data and processing activities associated within access management raises vulnerabilities and cyber concerns in privileged activities associated with sensitive data. Such unusual activities must be audited and framed around an audit risk model resilient to the transition of personal data privacy and security rights, in addition, to the new regulation. An effective control and legal framework is imperative in the preparation and interpretation of GDPR against business and IT framework designs. The various technical and business complexities which give rise to the levels of risk provokes an analysis of company policies and procedures during the planning phase, in which, should be tested to ensure controllers and processors are complying with data subjects' rights within the constraints set by GDPR.

Key Words: European Union, General Data Protection Regulation, risk management

Directive V. Regulation

1995: Data Protection Directive ("the Directive" or "Directive 95/46/EC")

The Directive is a regulation adopted by the European Union and based on recommendations proposed by the Organization for Economic Co-operation and Development's (OECD). The Directive protects the privacy of all personal data collected for or about citizens of the European Union (EU), especially in relation to processing, using or exchanging data. Any data in which an individual can be identified is at the sole responsibility of the data controller, i.e. owner of the data. The Directive is superseded by the General Data Protection Regulation (GDPR Report).

2018: General Data Protection Regulation ("GDPR")

GDPR was adopted by the European Parliament and European Council in April 2016 and became enforceable in May 25, 2018. The new regulation expands upon previous requirements for collecting, storing and sharing personal data, and requires the subject's consent to be given explicitly and restricts data privacy metrics. Enforcing the regulation as to a directive streamlines a transparent legal framework across all 28 EU countries.

A major change from the Directive is data processors being held accountable and responsible for data protection and privacy. Concern areas within cyber issues and third party contracts are highly risky in access management and processing activities (Schammo).

Introduction

The General Data Protection Regulation (GDPR) is a regulation requiring businesses to protect personal data and privacy of European Union (EU) citizens for transactions that occur within the EU Member States[1]. As stated, GDPR is a regulation, not a directive; it has a binding legal force. The objective of the new set of rules, implemented May 25, 2018[2], intends to give citizens more ownership over personal data and to simplify the regulatory environment for businesses. In the era of digitization, reforming into a standard of protection everywhere in the EU revolutionizes the framework in how and in what ways data is synthesized and analyzed (Hunton & Williams LLP).

Inside and outside territories that conduct business within the EU, encompassing all types of businesses, specifically internet-based business models, will be significantly affected. An organization established in the EU is subject to GDPR, which replaces the Directive and overrides national laws that implement the Directive, to the extent that these have not been reconciled. An organization outside of the EU is subject to GDPR under these conditions; offers goods or services to EU data subjects or monitors the behavior of EU data subjects. For example, activities in Member States, or in relation to residents of such Member State, which currently follows the Directive [Rec.20;Art.1(1)(c)][3] and uses means of processing in the EU will have low, if any, practical impact from the GDPR implementation. GDPR applies to organizations established outside the EU if the controller or processor processes personal data of EU residents when offering a good or services. Alternatively, any organization not currently under the Directive, but offers goods or services to EU residents, is subject to a full range of compliance obligations under GDPR (Gabel).

Who Is Classified As a EU Citizen?

Personal Data

The relevant processing activities by United States (US) companies are predominately affected by the outside impact of the EU GDPR regulation and must abide by extra territorial applicability. In consideration of the applicable organizations affected by GDPR outside the Member States and non-explicit subjectivity to the Directive, describing what and who constitutes as personal data, as well as other data classifications, within EU and US policies should be defined. Under [Rec.20; Art.2 (a)] of the Directive, *personal data* is defined as information relating to identifiable persons (i.e. "data subject"); directly or indirectly, in particular by reference to an identification number or to one or more factors specific to physical, physiological, mental, economic, cultural or social identity (Schammo). Under [Rec.26; Art. 4(1)] of the GDPR, the definition of *personal data* is similar to the Directive, with the exception, that the particular reference is an "identifier" such as an identification number, location data, and the online identifier specific to additional factors of "genetic" data (Schammo).

Sensitive Data

The special category of *sensitive data* within the classification of personal data is subject to additional protections, and organizations must have high grounds to process the data as to general personal data. Under [Rec.20; Art.8 (1)] of the Directive, *sensitive data* is personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and data concerning health or sex life (Schammo). Under [Rec.10 34, 35, 51; Art.9 (1)] of the GDPR, sensitive data is an extension of the Directive's description with data concerning health or sex life and sexual orientation; genetic data or biometric data. Data relating to criminal offenses and convictions under the criminal law adhere to outside of EU legislative competencies. The GDPR makes no material alterations to the approach set out by the Directive.

---

[1] The EU consists of 28 member states founded by the union and is subject to the privileges and obligations of membership. Following the 2017 International Monetary Fund data report, to list a few Member States, as provided by ascending nominal GDP per capita (in billion USD) are; Germany (*$3,651,871*), France (*$2,574,807*), United Kingdom (*$2,565,810*), Italy (*$1,921,139*), Russia (*$1,469,341*), and Spain (*$1,307,170*). *International Monetary Fund, World Economic Outlook Database (IMF, October, 2017).*

[2] *EU General Data Protection Regulation, GDPR Timeline of Events (EUGDPR, 2018).*

Anonymous Data

Individuals in which cannot be identified, directly or indirectly, to data are defined as *anonymous data*. Under [Rec.26] of the Directive and [Rec.2] of the GDPR, there is no clear applicability to anonymous classifications to data (Schammo). *Anonymous data* is outside the scope of the Directive and GDPR.

Pseudonymous Data

A special category of *pseudonymous data* within personal data is characterized as data which no individual can be identified, directly or indirectly, unless a "key" is defined to re-identify the data. Pseudonymization does not remove all identifying information from data, yet reduces the likability of a dataset with the original identity of an individual (e.g., an encryption scheme). Organizations with personal data should implement one or more of the following techniques to minimize risk and automation can reduce the cost of compliance: data masking and data encryption. Data masking is a more widely applicable standard solution as it enables organizations to maintain the usability of their customer data (Schammo).

Additionally, data can be de-identified and de-sensitized so that personal information remains anonymous in the context of support, analytics, testing, or outsourcing. On the other hand, data encryption translates data into another form, or code, so that only people with access to a secret key, a "decryption key," or password can read it. Under [Rec.26, 28-29, 75, 78, 156; Art.4(5), 6(4)(e), 25(1), 32(1)(a), 40(2)(d), 89(1)] of the GDPR, *pseudonymous data* is treated as personal data because it enables the identification of individuals via a key. The key enables re-identification of individuals to be kept separate and secure. The risks associated with pseudonymous data are lower. Therefore, the levels of protection required for such data are lower (Schammo).

Processing Activites

Processing is a vague term which encompasses any personal data, including collecting storing and deleting such data. Under [Art.2 (b)] of the Directive, processing means any operations performed within the scope of personal data, automatic or not; in the forms of collecting, recording, organizing, storing, adapting, altercating, retrieving, consulting, using, disclosing, disseminating, blocking, or destructing the data (Schammo). Under [Art. 4(2)] of the GDPR, the characteristics of processing activities are similar as the Directive, with the exclusion, performing upon personal data or 'sets of personal data.' Relative to the Directive, implementing GDPR will not give rise to a significant impact on what is defined as the current state of processing activities.

Data Protection and Privacy

Data Subject Rights

An effective security plan, with resilient breach response modifications, builds an infrastructure willing and able to transform into the paradigm data transparency shift. The role of the controller and processor is vital in the preparation and interpretation of the new regulation against current business and IT framework designs. Policies and procedures designed should be tested continuously to ensure controllers are able to comply with data subjects' rights within the time limits set by GDPR. Controllers should review and update current fair collection notices to guarantee compliance with the extended information requirements. It is imperative to discuss the various data subject rights with significant changes from the Directive to the GDPR in light of controller and processor responsibilities in the new age of data transparency and empowerment (Loshin).

Breach Notification

Prior to the anticipated GDPR implementation, Europe had no universally applicable law requiring notification of data breaches. Under [Art. 33(1)] of the GDPR, "the controller without undue delay, and where feasible, not later than seventy-two hours after having become aware of it, shall notify the breach to the supervisory authority." Companies are required to build an infrastructure resilient and automatically responsive in compliance to the EU enforced standard. Failure to comply, in relation to security and data breach notification, can amount up to ten million Euros for the controller and processor. The role of the controller and processor is highly important in the interpretation and practice of the new regulation. Controllers are required to implement appropriate technical and organizational measures together with a process for regularly testing, assessing and evaluating the effectiveness of those measures to ensure the security of processing [Article 32]. Therefore, implementing a coordinated approach, including technology, enforces breach response policy and broader staff training making employees ready and able to respond to data breaches and report as quickly as demanded by the regulation.

Controllers are also required to keep a record of all data breaches, whether or not notified to the supervisory authority, and permit audits by the supervisory authority [Article 33(5)]. Employees represent a highly probable security source as to technology. Regular training raises awareness and importance in good security practices and how to identify current threats. Dependent on a corporate network's applications, developing a modified plan with an effective breach response tactic requires a combination of information technology, personal relations and legal (Hunton & Williams LLP).

Other Data Rights For Individuals

Right to Access

Expanding from the GDPR, within [Article 15], right for data subjects to obtain from the data controller confirmation as to whether or not personal data concerning them is being processed, where and for what purpose. Meaning, the controller must provide a copy of the personal data, free of charge, in an electronic format. The subject access rights dramatically changes into a paradigm of data transparency and empowerment of data subjects (Gabel).

Right to be Forgotten

Under [Article 17], the right to be forgotten, or "data erasure," warrants the data subject to have the right for the data controller to erase personal data, terminate further dissemination of the data, and potentially have third parties halt processing of the data. The conditions for erasure, includes data no longer being relevant to original purposes for processing, or a data subjects withdrawing consent. Also, requiring controllers to compare the subjects' rights to "the public interest in the availability of the data" when considering such requests. This right is not absolute because it only raises a narrow set of processing circumstances where the controller has no legal ground for processing the information (Gabel).

Right Not to be Subject to Automated Decisions

Expanding from the Directive right not to be subject to automated decision making, GDPR expressly refers to profiling as an example of automated decision making [Article 22]. Automated decision making and profiling "which produces legal effects concerning, the data subject, or similarly significantly affects are only permitted where; one, necessary for entering into or performing a contract, two, authorized by EU or Member State law, and three, the data subject has given their explicit consent." The scope of this right is potentially broad and may throw into question legitimate profiling (e.g., to detect fraud and cybercrime). It also presents challenges for the online advertising industry and website operators who will need to revisit consenting mechanics to justify online profiling for behavioral advertising (e.g., cookies and online tracking). (Gabel).

Data Portability

New to GDPR and no deviation from the Directive, under [Article 20], processing of personal data is justified on the basis that the data subject has given their consent to processing or where processing is necessary for the performance of a contract. As well as, where the processing is carried out be automated means, and the data subject has the right to receive or transmit to another controller all personal data. Again, it is imperative that controllers develop procedures to enable the collection and transfer of personal data when requested to do so by data subjects and fall within legal and control framework metrics (Gabel).

Hot Topic: Cybersecurity

The more control one has over who has access to sensitive and confidential data, the more control you have over how much damage can be done when a user account is used for malicious activity. Sounding easier said than done, this concept enforces the protection of data against the numerous calculated and uncalculated threats. Because remediation and loss of business are two of the biggest costs one faces after a data breach, being able to limit what is leaked can keep your business operating productively and effectively. Indicative by the substantial growth of an expected twelve-fifteen persent CAGR (compound annual growth rate) with a five year trailing projection, anticipating the fines for non-compliance aggravates the demand for identity and access management (IAM) spending. According to a 2017 Ovum report, an anticipated two-thirds of U.S. companies will be affected by GDPR. Therefore, this will require them to restructure their business and IT-focused strategies in EU countries (EU GDPR Portal).

Access Management

A form of an access management solution to cyber concerns is the identity and access management (IAM), which is a framework for business processes that facilitates the management of electronic or digital identities. The framework includes the organizational policies for managing digital identity, as well, as the technologies needed to support identity management. Hence this aligns business and information technology within the company's infrastructure design (Loshin).

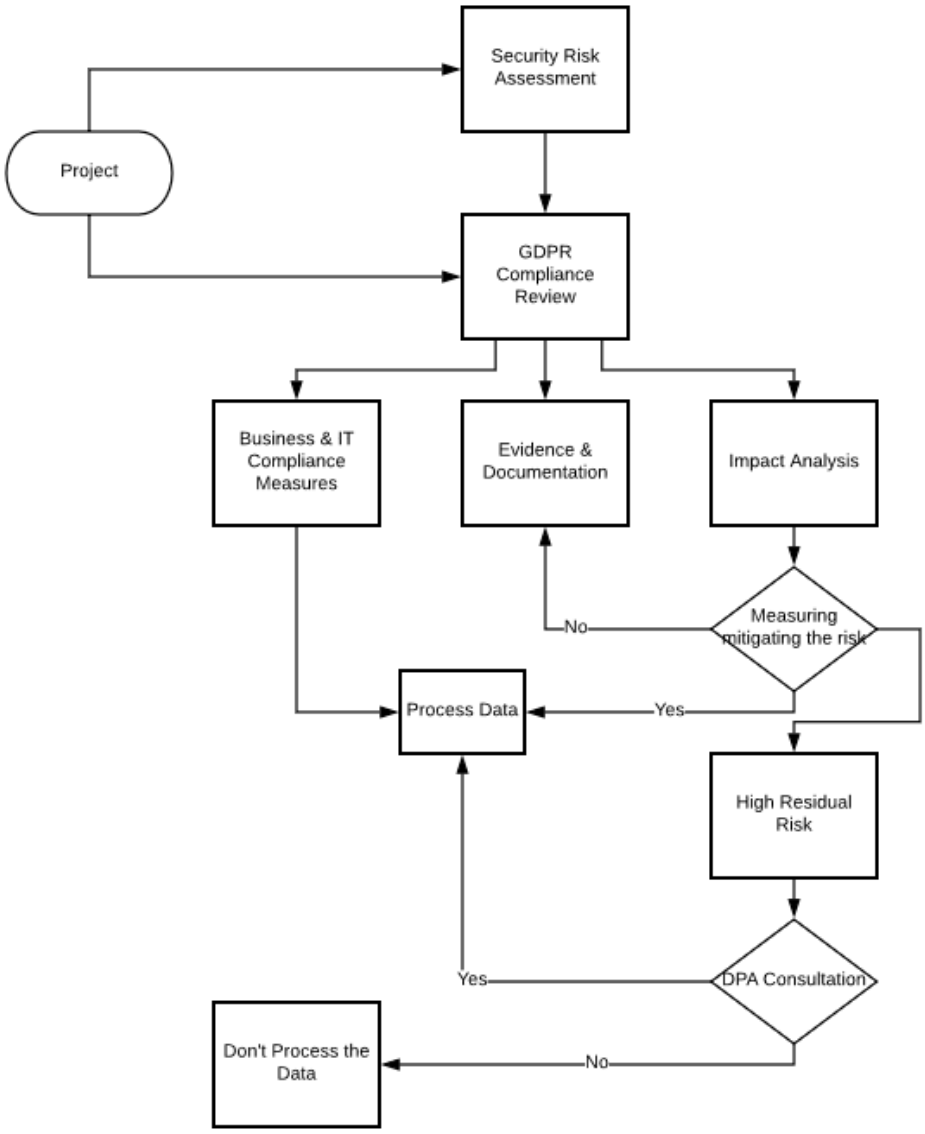
Privileged and Sensitive Data

Protecting personal data requires complete control over privileged access, which is the foundational principle of the GDPR. Controllers and processors will be required to assess risks posed by personal data processing operations to the rights and freedoms of individuals. GDPR [Article 32(1)], as the "security of processing"; provides that controllers and processors must consider' among various external and internal factors, the risks to the fundamental rights and freedoms of individuals that are associated with their processing activities and must implement "appropriate technical and organizational measures to ensure a level of security appropriate to the risk". Article 40 (2)(h) provides the codes of conduct in which addresses risk assessments and sanctions the accountability and governance metrics organizations must adhere to within their governance, compliance and technology internal frameworks (Hunton & Williams LLP).

The "Risk-Based Approach"

A "risk-based approach" follows the practical application of the GDPR within an organization's internal framework; across governance, compliance and technology through accountability and internal privacy management programs. Risk can be classified by taking into account the time frame of the impact of the possible harms and subsequent threats to security of the organization. Solutions and opportunities for policy development and guidance on key implementation issues expand the risk-based approach within GDPR compliance complexities (e.g., processing activities giving high risk across business operations). Through risk management practices, following the risk identification and classification system is useful as it enables organizations to define the scope of risk management within their organizations and to have a repeatable and consistent framework to identify risks to individuals in case by case scenarios over time.

Figure 1
Stages of the Risk Assessment Process in Compliance to GDPR Data Processing



In consideration of how controllers respond or in what ways it affects management review of their practices captures the effect on the audit whether or not to process the data and seek consultation to connect technological risk to system design, which is identified by the process flow above (*Figure 1*).

Risk Assessments

In application to assessing risk within the business and IT process functions within an organization's infrastructure, utilizing an "Audit Risk Model" classifies and maps the direct and indirect relationships from *Figure 1's* process design flow.

Table 1
Risk Tolerance Levels under GDPR in Practice

#	Activity	Impact on Business Objective (Risk Level)	Likelihood	Description
1	Large scale processing of sensitive personal data	High		
2	Automated profiling	High		
3	Systematic monitoring	High		
4	New data processing technologies	High		
5	CCTV monitoring of public spaces	High		
6	Processing sensitive personal data	Medium		
7	Processing personal data of vulnerable individuals	Medium		
8	Large scale processing of personal data	Medium		
9	Anonymized data	Low		
10	Pseudonymized data	Low		
11	Secure small scale processing	Low		

The above matrix organizes the level of risk on a situational basis. The likelihood is the possibility or probability of occurrence. The description is the detail and explanation of the relative impact on the business or information technology process.

Conclusion

Defining the main changes from the Directive to GDPR is imperative in the discussion of how, who, what, and why data is captured and the relative impact on business and information technology processes within an organization. Additionally, an integral perspective is the transparency of data and empowerment of individual users. In audit practices, access management is a high risk area especially now under GDPR changes to privileged access. The financial services base will need to develop an effective security plan with robust breach response variations, while building an infrastructure willing and able to transform into the data transparency shift paradigm. Personal data and processing activities associated within access management raises vulnerabilities and cyber concerns in privileged activities associated with sensitive data. Henceforth, an effective control and legal framework is imperative in the preparation and interpretation of GDPR against business and IT framework designs.

Bibliography

Gabel, Detlev. “Preparing for the GDPR – Unlocking the EU General Data Protection Regulation.” White & Case, White & Case LLP, 22 July 2016.

GDPR. “Data Masking: Anonymization or Pseudonymization?” GDPR.Report, 28 Sept. 2017.

Hunton & Williams LLP. “Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR.” Centre for Information Policy Leadership, 21 Dec. 2016, pp. 1– 44.

“Key Changes with the General Data Protection Regulation.” EU GDPR Portal, Trunomi, 2016.

Loshin, Peter. “The GDPR Right to Be Forgotten: Don't Forget It.” SearchSecurity, TechTarget, 27 July 2017

Schammo, Pierre. “EU Prospectus Law by Pierre Schammo.” Cambridge Core, Cambridge University Press, 2011.

United States, Congress, Regulation (EU) 2016/679 of the European Parliment and of the Council. Official Journal of the European Union, 2016.