The General Data Protection Regulation

PPAI White Paper • January 2018

This white paper has been prepared for informational purposes only and does not constitute legal advice. To learn more about the upcoming General Data Protection Regulation, consult your legal counsel or visit: www.eugdpr.org

OVERVIEW

Data can be described as the lifeblood of today's economy. Through the years, its intrinsic value has evolved into a critical asset for business growth and competitiveness. And yet, the opportunity that data presents also comes with great risk and responsibility. Many battle over who should own and benefit from data, consequently elevating the need for privacy protection and stringent standards. What was once a business-practice afterthought is about to be elevated in importance by a new piece of legislation out of the European Union (EU), bringing data protection to the forefront for virtually any company.

The General Data Protection Regulation, more commonly known as the GDPR (Regulation), took over four years of development and discussion until its adoption in April 2016. The GDPR was designed to protect EU citizens in an increasingly data-driven world, vastly different from the time the Data Protection Directive (DPD, Directive) was established in 1995, when the internet was still in its infancy. The current Directive was adopted in 1995 and went into effect in October 1998. For more than 20 years, the DPD has served as the basic instrument for data protection in the EU, recognizing privacy as a fundamental human right.

> **"It is paramount to understand how the GDPR will change not only the European data protection laws, but nothing less than the whole world as we know it."**
>
> **– Jan Philipp Albrecht**[1]

BACKGROUND

The original concept of 'privacy' was developed in 1890 by U.S. judges Samuel D. Warren and Louis D. Brandeis in their *Harvard Law Review* article, "The Right to Privacy."[2] The article established the right "to be let alone" and in the context of privacy, it means not to be viewed in any way other than how the individual chooses to be viewed; "privacy is the ability to be yourself." Warren and Brandeis laid the foundation that has since been carried into modern regulations on the concept of privacy.

In modern times, the distinction between public and private information is similarly critical for a functioning democracy and is afforded protection in constitutional instruments. Privacy enables individuals to engage in the process of democracy by providing space to form thoughts and to interact socially and politically with others. Against this background, the invasion of privacy may lead to situations in which personal data is withdrawn from society even with societal interest. Accordingly, privacy depends on the political ideology that dominates a specific society and as such, require protection. Data protection rules make it possible to use personal data in an acceptable manner in society. The concepts of 'privacy' and 'protection' both strive to ensure the autonomy and integrity of individuals; however, the legal safeguards rely on the individual as part of society. The concept of privacy as a tool facilitates individual opacity and protects against intrusion, while data protection promotes transparency and accountability.[3]

The World Has Moved On Since 1995

The Data Protection Directive (DPD) was adopted in a world very different from the one in which we live today. The World Wide Web, which was previously available only to the government and universities, had only just become publicly accessible.

Rich streams of data continuously grow in size, pace and accessibility, feeding flows of information, innovation and opportunity into an already cloudy ecosphere. Where once data was captured and used once for a concrete purpose, today, many times the latent value is unclear at the time data is collected and can only be fully acquired if the data is reused or combined with data sources. This shift creates a very strong economic incentive in how data is being handled: it will be collected whenever possible, even when no concrete use case is evident; collection is opportunistic rather than purposeful. Similarly, there is an equal economic incentive to keep the data for as long as possible. The widespread circulation of data has led to massive privacy concerns. The constant evolution of technology creates tools that enable corporate actors to market communicate in a much more specific and accurate way: the same user is reached[4] across multiple devices.[5]

Technology has enabled personal data to be more transparent. The Internet and network ecosystem erase the border between public and private information. The overexposure of citizens weakens their trust and commitment to law minimizes the checks and balances on the exercise of government power. Dan Solove notes in his book, *Understanding Privacy*, that "privacy may be implicated if one combines a variety of relatively innocuous bits of information. Businesses and government often aggregate a wide array of information fragments, including pieces of information we would not view as private in isolation. Yet when combined, they paint a rather detailed portrait of our personalities and behavior." Technologies and routine commercial uses expand the public sphere while simultaneously neglecting the expectations of privacy. This kind of transparency coupled with ubiquitous data collection and ambient surveillance, creates a subtle, but fundamental challenge to governance through the rule of law both domestically and internationally.[6] While the DPD provided a solid foundation, it was not equipped to handle the explosion in data. We are in a new age. And we need new rules.

The GDPR was designed to embrace the new digital environment by giving individuals control over their personal data, and simplifying the regulatory environment for business. The data protection reform enables both EU consumers and businesses to benefit in a new economy.

> **17 years ago, less than one percent of Europeans used the internet. Today, vast amounts of personal data are transferred and exchanged, across continents and around the globe in fractions of seconds. The protection of personal data is a fundamental right for all Europeans, but citizens do not always feel in full control of their personal data. My proposals will help build trust in online services because people will be better informed about their rights and in more control of their information. The reform will accomplish this while making life easier and less costly for businesses. A strong, clear and uniform legal framework at EU level will help to unleash the potential of the Digital Single Market and foster economic growth, innovation and job creation.**
>
> -Viviane Reding, EU Justice Commissioner & European Commission Vice President
> Announcement Of European Data Protection Reforms, January 2017[7]

EU LAW

The European Union (EU) as was created by the Maastricht Treaty, formally known as the Treaty on European Union (TEU) in November 1993.8 According to its website, the objectives of the EU are to establish European citizenship, ensure freedom, justice and security, promote economic and social progress, and assert Europe's role in the world.[9] In 2012, the EU was awarded the Nobel Peace Prize "for over six decades contributed to the advancement of peace and reconciliation, democracy and human rights in Europe"[10] Today, the EU represents 28 countries known as 'Member States' (see page 25 for more information).

The EU was set up as a 'community of law' as stipulated in Article 2 of the TEU, and it operates under a single market to allow the free movement of goods, capital, services and people. EU law was given precedence over national law and direct effect, as evidence of the significance of mutual trust among its member states and their respective legal systems.[11] The 'life cycle' of EU law, including its creation, application, interpretation and enforcement, involves various formal actors referred as the EU Institutions. Key roles are played by the Commission, Parliament and Council (see page 26 for more information).[12]

EU law is divided into 'primary' and 'secondary' legislation. 'Treaties' constitute ***primary legislation***, which is comparable to U.S. constitutional law at the national level.[13] The treaty regarding the protection of individuals with regard to automatic processing of personal data was signed as "Council of Europe Convention 108" and went into effect in October 1985.[14]

The principles set forth by the EU treaties are carried out through 'binding' and 'non-binding' legal acts known as ***secondary legislation***. These legal acts are identified in Article 288 of the Treaty on the Functioning of the European Union.[15] The binding legal instruments that make up the secondary legislation are 'regulations,' 'directives' and 'decisions.' The non-binding legal instruments that make up the secondary legislation are 'recommendations' and 'opinions.'

A *regulation* is binding in their entirety, directly applicable in all Member States as soon as they enter into force. They are designed to ensure the uniform application of *community law* in all the Member States and therefore do not need to be transposed into national law. Regulations supersede national laws incompatible with their substantive provisions. In principle, a *directive* is binding, though not directly applicable, unlike regulations. Member States must guarantee the effectiveness of EU law, in accordance with the 'principle of sincere cooperation' established in Article 4(3) TEU, by adopting a implementing measure to 'transpose' the directive into State law in line with national objectives. In European Union law, *transposition* is a process by which the European Union's member states give force to a directive by passing appropriate implementation measures.[16]

From Directive To Regulation

On May 25, 2018, the General Data Protection **Regulation** (Regulation (EU) 2016/679) will replace the Data Protection **Directive** (Directive 95/46/EC). Many principles and characteristics of the DPD are retained in the GDPR; however, it is important to identify the differences in order to better interpret and understand the significance of the upcoming regulation.[17]

THE GENERAL DATA PROTECTION REGULATION

The General Data Protection Regulation is formally known as **Regulation (EU) 2016/679**, though commonly referred as the GDPR. The complete text contains 99 articles and 173 recitals within 88 pages.

Over Four Years, Over 4,000 Amendments

Since the first proposal of the GDPR was introduced in January 2012, there have been more than 4,000 amendments, making the GDPR the most lobbied regulation in the history of the European Parliament.[18] After four years of heavy political debate and intense industry lobbying, the final text was agreed upon in December 2015 and published in the *Official Journal of the European Union* in May 2016. While previous drafts of the proposed legislation suggested extreme measures, the final draft is perceived as commercially balanced, and can be seen as an evolution of the current law rather than a revolution.

The first 31 pages include the *preamble*, which defines the legal basis of the regulation. The remaining pages provide the enacting terms, which are defined under the 99 articles and their corresponding recitals of the GDPR. The *recitals* are generally written to be used by the Court of Justice of the European Union (CJEU) in order to establish meaning "of the enacting terms of an act."[19] The recitals provide additional information to supplement the articles with related context, as well as essential information for effectively implementing the GDPR. The 173 recitals are important to ensure complete compliance with, and understanding of, the regulation.

ARTICLES	RECITALS
The Rules	*Background & Objectives*
99	173

Article 29 Establishes A Working Party

Articles 29 and 30 of the DPD established an advisory body, known as Article 29 Working Party (WP29), to: "(i) examine any question covering the application of the national measures adopted under this Directive in order to contribute to the uniform application of such measures; (ii) give the Commission an opinion on the level of protection in the Community and in third countries; (iii) advise the Commission on any proposed amendment of this Directive, on any additional or specific measures to safeguard the rights and freedoms of natural persons with regard to the processing of personal data and on any other proposed Community measures affecting such rights and freedoms; (iv) give an opinion on codes of conduct drawn up at Community level."[20]

The European Commission hosts a website maintaining material (opinions, recommendations, guidelines, working documents, letters, etc.) issued by the WP29 in accordance to the policy mandating any correspondence recorded as such.

WP29 Becomes The EDPB

Under the newly adopted regulation, WP29 will become the European Data Protection Board (EDPB) as a "body of the Union," as described in Article 68 in the GDPR. Much like the WP29, the EDPB has advisory status and acts independently; however, the question still remains whether the EDPB is more than simply a rebranding of the WP29.

Since its adoption, the WP29 has published a number of guidelines on how to interpret and implement the forthcoming GDPR, outlined in the 2016[21] and 2017[22] GDPR Action Plans. In December 2016, the WP29 published guidelines on *The Right To Data Portability*,[23] *Data Protection Officers ('DPOs')*[24] and *Identifying A Controller Or Processor's Lead Supervisory Authority*.[25] In 2017, the WP29 has released guidelines on *Data Protection Impact Assessment (DPIA)*[26] in April, *Data Breach Notification*[27] in October, *Consent*[28] in November and *Transparency*[29] in December. In June, the WP29 also published their Opinion on *Data Processing At Work*.[30] Though the material under the GDPR seems consistent with the guidelines and opinions under the DPD, there are several provisions in the regulation that state the EDPB has the final say. This indicates an administrative restructuring of the WP29 to become a more prominent body.

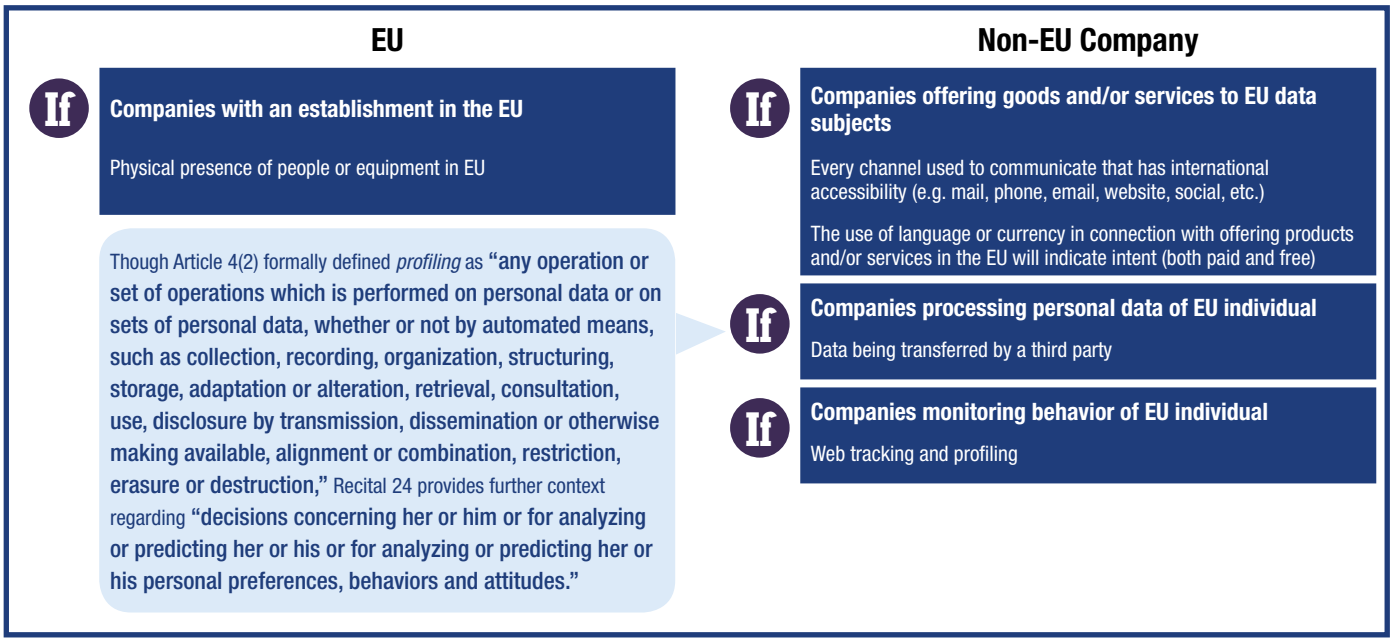
A CLOSER LOOK

Who Must Comply?

The GDPR applies to companies involved in the 'processing' of 'personal data' of Data Subjects located in the EU. The regulation defines ***processing*** as "any operation or set of operations which is performed on personal data or on sets of personal data" and ***personal data*** as "any information relating to an identified or identifiable natural person." These broad definitions encompass a range of data types and uses discussed in more detail on page 9.

Companies involved in processing personal data are divided into two categories: 'data controllers' and 'data processors.' A ***data controller***, "determines the purposes and means of the processing of personal data." A ***data processor*** on the other hand, "processes personal data on behalf of the controller." Though these definitions remain largely unchanged, the GDPR significantly expands the territorial reach of EU legislation, applying its requirements to three specific categories of entities (Figure 1).

Figure 1. How To Determine If You're Within The GDPR Scope



Companies, including those in the U.S., that fall within any of these categories will be required to comply with the list of obligations imposed by the GDPR. These categories and the related implications will be discussed on page 10.

These obligations can be organized into three different streams: **(i.) data principles**, **(ii.) data subject rights**, and **(iii.) accountability**. Many of these obligations are a continuation of those established by the 1995 EU Directive, but others are either new or expanded.

Figure 2. Key Changes Introduced By The GDPR

The GDPR transforms a number of existing requirements and introduces a host of new ones that are likely to require significant changes in the way data is managed throughout a company.

	Data Protection Directive (DPD) Directive 95/46/EC	General Data Protection Regulation (GDPR) Regulation (EU) 2016/679
Number Of Chapters; Articles	VII; 34	XI; 99
Objective	Safeguard free movement of personal data through a common market	Revise a legal framework that could cope with future data processing and privacy challenges. Repeals Directive 95/46/EC.
Legislation Effect	Enabling legislation; varying regulations in EU countries	Binding regulation; directly enforceable in all EU countries
Geographic Reach	Emphasis applied to location of processing; if equipment on EU territory	Emphasis applied to data subject; if an EU resident
Liability	Only data controllers held liable	Both data controller and data processors are liable
Definitions	The definition of 'personal data' includes: Name Photo Email Address Phone Number Address Personal Identification Numbers	The definition of 'personal data' extended to include: IP Addresses Mobile Device Identifiers Geo-Location Biometric Data Psychological IdentityGenetic Identity Economic Status Cultural Identity Social Identity
Rights	Data subjects granted: the right of access the right to erasure ("be forgotten") the right to object the right to rectification	Data subject rights extended to include: the right to restriction of processing the right to data portability
Consent	Potential to rely on 'implicit' consent depending on jurisdiction	Required to gain unambiguous consent (i.e. explicit)
Transparency	No requirement to maintain personal information inventory	Organizations will need a personal information inventory
Data Protection Officer (DPO)	Voluntary DPO regime	DPO must be appointed when core activities involve regular and systematic monitoring of data subjects on a large scale
Enforcement	Supervisory authorities' (SA) have limited powers under national law	SA's will be given a wider range of authority
Fines	Fines vary by jurisdiction	Regulators can impose fines up to €20 million (roughly $23.5 million) or four percent of a company's global annual income, whichever is higher
Breach Notification	No obligation to report breach	DPO required to report breach within 72 hours

Territorial Scope

Article 3.

The GDPR extends, modernizes and clarifies the jurisdictional scope of the existing EU data protection law.

(1) This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

First, a controller or processor that maintains an 'establishment' in the EU will be subject to the GDPR if it processes personal data in the context of that EU establishment, regardless of whether the processing actually takes place in the EU. While the term *establishment* is not explicitly defined, Recital 22 explains that "effective and real exercise of activity through stable arrangements" will satisfy the provision. Additionally, "the legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect." In other words, the regulation may apply even if a company's nexus to the EU is less formal than a parent-subsidiary relationship.

(2) This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union.

Second, a controller or processor not established in the EU will be subject to the GDPR "where the processing activities are related to offering goods or services to data subjects in the Union," even when the goods and services are offered free of charge. Products and/or services provided in exchange for marketing (e.g. promotional products) are just as much in scope as products and/or services provided in exchange of contracts and invoices. This is a key change in the data protection law: the relevance of the equipment location is replaced by a focus on the people in the EU.

(3) This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to (b) the monitoring of their behavior as far as their behavior takes place within the Union.

Third, a controller or processor not established in the EU will be subject to the GDPR if it processes the personal data of Data Subjects in the EU and that processing is related to the 'monitoring' of the behavior of data subjects taking place within the EU. In this case, Article 27 indicates the requirement to appoint representatives in the Union or more specifically, in the concerned Member State.

DEFINITIONS

The DPD was not nearly as expansive in its geographical reach due, in part, to the stipulated definition of 'personal data' portrayed in this era.[31] The directive defined personal data as "any data relating to identified or identifiable natural person," known as the 'data subject,' meaning anyone "who can be identified directly or indirectly" by reference to "an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity." More extensive guidance was given in the Article 29 Working Party (WP29) Opinion 4/2007 On The Concept Of Personal Data.[32] The GDPR accepts the definition of personal data used by the DPD, while including additional examples (emphasized in blue):

Personal Data

DPD, Article 2(a).

Personal Data shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

GDPR, Article 4(1).

Personal Data means any information relating to an identified or identifiable natural person 'data subject'; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

The definition of *Personal Data* in both the DPD and the GDPR comprises three main points: it is 1) 'any information,' related to 2) a 'natural person' who is 3) 'identifiable.' In the context of technological development, the identifiability factor proves to be the most pertinent. A natural person can be considered 'identified' when he or she is distinguished from all other members of a group. In other words, data will usually not be personal if they can only be linked to a group of persons as opposed to one single person.[33] Respectively, a natural person is 'identifiable' when that person has not yet been identified but identification is possible. The possibility of identification therefore forms a threshold for determining whether information is personal data and within the scope of the GDPR and thus, the mere possibility of identification can be enough for data to become personal information. Identification is generally achieved through *identifiers*, or specific attributes linked to an individual.

The GDPR expands the list of examples to include 'names,' 'identification numbers,' 'location data' and 'online identifiers.' The use of "such as" emphasizes that these identifiers are non-exhaustive. *Location* data is not specifically defined, but it is associated with data that has any kind of geographic position attached to it. This is classified as 'personal' because it could be used to identify where an individual lives, works, and sleeps, or to find out social, religious or cultural identities. *Genetic* data specifically refers to gene sequences, which are used for medical and research purposed. Article 4(13) defines *genetic data* as "relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question." Recital 34 provides further context indicating "inherited or acquired genetic characteristics of a natural person which result from the analysis of a biological sample from the natural person in question, in particular chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis, or from the analysis of another element enabling equivalent information to be obtained are classified as genetic data."

Special Categories Of Personal Data

Article 9(1).

Article 9 prohibits the processing of certain types of data labeled as special categories.

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

Article 4(14) defines *biometric data* as "personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data. Article 4(15) then clarifies data concerning *health* as "personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status."

The revised definition was written to be technology neutral and therefore future-proof. The rationale for this approach is the desire of the EU parliament to ensure that the protection afforded by the GDPR is not circumvented with the aid of technology.

Personally Identifiable Information (PII)

'Personal Data' does not carry the same meaning as *Personally Identifiable Information* (PII), a term mostly used in the United States. According to National Institute Of Standards And Technology (NIST), PII is:

Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.[34]

Personal Data Is PII+

According to the Mobile Marketing Association, *Non-PII* is "information that may correspond to a particular person, account or profile, but is not sufficient to identify, contact or locate the person to whom such information pertains; non-qualified lead." Examples of this are: device IDs, IP addresses, cookies, language preference, time zones.

In the context of the GDPR, the distinction between PII and Non-PII is irrelevant, because new examples that have been added to the definition of Personal Data share examples of Non-PII. Therefore, it can be argued that all PII data is Personal Data, but not all Personal Data is PII data.

Data Subject

Article 4(1).

The regulation brings a perceptible shift from territory to personality as a basis for jurisdiction. This is evidenced by the changing nature of data controller and data processor obligations and the increased emphasis on data subjects. The data subject is a neutral person whose personal data is processed by a processor or controller.

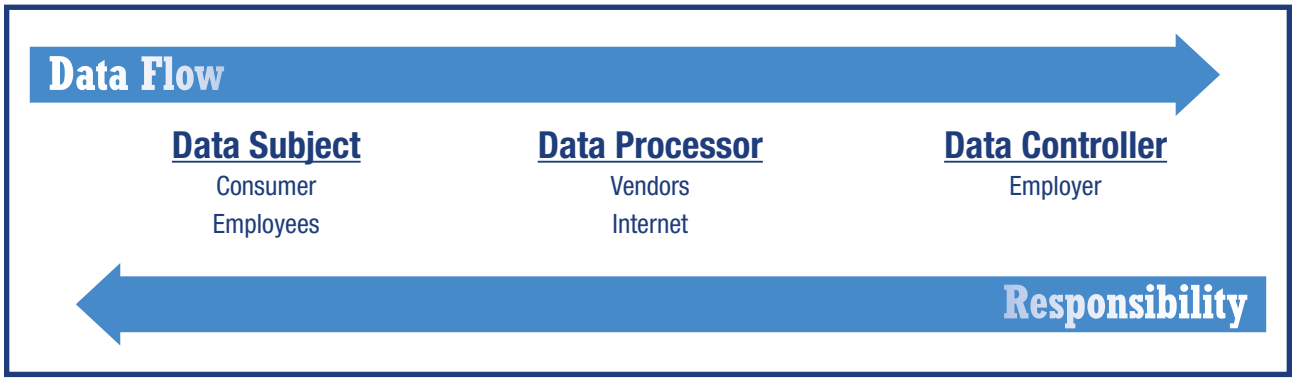
The wording "data subjects who are in the Union" under Article 3(2) is quite deliberate. The GDPR covers data processing of individuals on EU territory, including citizens, temporary residents and even those on vacation or in transit (e.g. airport layover).

Processing

Article 4(2).

'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Figure 3.



THE RULES TO DATA PROCESSING

Article 1(1)

This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.

These rules can be found under Article 5 of the GDPR, similar to the ones established in Article 6 of the DPD, as the fundamental "principles relating to processing personal data."

Figure 4. Principles Related To Processing Personal Data

		DPD	GDPR
		Principles Relating To Data Quality **Article 6.**	**Principles Relating To Processing Of Personal Data** **Article 5.**
1.		Member States shall provide that personal data must be:	Personal data shall be:
(a).	**Lawful, Fair & Transparent**	processed fairly and lawfully; Recital 38	processed lawfully, fairly and in a transparent manner in relation to the data subject; Recital 39
(b).	**Purpose Limitation**	collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards; Recital 28	collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, **in accordance with Article 89(1)**, not be considered to be incompatible with the initial purposes; Recital 50
(c).	**Data Minimization**	adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed; Recital 28	adequate, relevant and **limited to what is necessary** in relation to the purposes for which they are processed; Recital 39
(d).	**Accuracy**	accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;	accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay; Recital 39
(e).	**Storage Limitation**	kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.	kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes **in accordance with Article 89(1) subject to implementation of the appropriate technical and organizational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject**; Recital 39
(f).	**Integrity & Confidentiality**	**Security Of Processing** **Article 17(1)** Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected. Recital 46	processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures; Articles 24(1), 25(1-2), 28, 39, 32; Recital 29
2.	**Accountability**	It shall be for the controller to ensure that paragraph 1 is complied with.	The controller shall be responsible for, and **be able to demonstrate** compliance with, paragraph 1. Recital 85

Data Principles

Lawfulness, Fairness and Transparency

Article 5(1)a

Article 6(1) identifies lawful basis for processing personal data when there is (a) consent, (b) contract, (c) legal obligation, (d) vital interest, (e) public interest or (f) legitimate interest.

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
(c) processing is necessary for compliance with a legal obligation to which the controller is subject;
(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. It is important to note that there is no hierarchy of the lawful basis for processing personal data and the most appropriate basis will depend the purposes for processing.

Relevant References: Articles 6, 9, 10 / Recitals 39, 45, 50, 63

The grounds for *fair* processing requires informing data subjects of the existence of the processing activities and its purposes at the moment of collection. The data subject must also be informed of the existence of profiling and consequences, if applicable.

Relevant References: Article 6 / Recitals 39, 45, 60, 71

While not explicitly defined in the GDPR, *transparency* takes the form of specific requirements found in later articles. Article 12 provides general rules on transparency, which apply to the provision of information (Articles 13-14) and communications with data subjects concerning their rights (Articles 15-22) and in relation to data breaches (Article 34). The principle of transparency requires that any information and communication concerning the processing of personal data must be easily accessible and easy to understand, and that clear and plain language be used. More specifically, this principle ensures data subjects receive information on the identity of controllers and purposes of the processing of personal data. Data subjects should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing.

Relevant References: Articles 12-22, 34 / Recitals 39, 58-63, 71

Purpose Limitation

Article 5(1)b

The principle of *purpose limitation* can be broken into two main ideas: (1) personal data may only be collected for specified (defined), explicit (clear) and legitimate purposes (legal basis) determined at the moment of collection and (2) personal data must only be processed in a manner compatible with those purposes, otherwise, it is required to establish a new and separate legal basis. There are also two exemptions to this principle: (1) under Article 89(1), processing for archiving, scientific, historical or statistical purposes as far as appropriate technological and organizational measures are in place to protect the rights and freedoms of the data subjects, in particular, the principle of data minimization and (2) under Article 6(4), processing for another purpose compatible with the purpose for which the personal data are initially collected. To assess compatibility, the following points should be considered:

(a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;
(b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;
(c) the nature of the personal data, in particular whether special categories of personal data are processed, or whether personal data related to criminal convictions and offenses are processed;
(d) the possible consequences of the intended further processing for data subjects;
(e) the existence of appropriate safeguards, which may include encryption or pseudonymization.

Relevant References: Article 6 / Recitals 39, 45, 50

Data Minimization

Article 5(1)c

The principle of *data minimization* requires personal data to be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. To limit the storage of the personal data to a strict minimum, there is a need to establish time limits for storing and deleting data or for conducting periodic reviews to assess what should be deleted.

Relevant References: Article 25 / Recitals 39, 156

Accuracy

Article 5(1)d

The principles of *accuracy* imposes the responsibility to take every reasonable step to ensure that personal data are accurate and up to date concerning the specific purposes for which they are processed. Inaccurate data shall be erased or rectified without delay.

Relevant References: Article 18 / Recital 39

Storage Limitation

Article 5(1)e

The principle of *storage limitation* refers to the obligation to keep the personal data as far as necessary to identify the data subjects for the purposes established. In that sense, the data retention has to be scheduled in a way that personal data is erased when the purposes have been served. The GDPR introduces two important new factors: (1) there are specific provisions on the processing of personal data for historical, statistical or scientific purposes under Article 89(1), and (2) the principle should be read in light of the "right to be forgotten," under which data subjects have the right to erasure of personal data, in some cases sooner than the end of the maximum retention period.

Relevant References: Articles 6, 23, 25 / Recitals 39, 45

Integrity and Confidentiality

Article 5(1)f

The principles of *integrity and confidentiality* require that appropriate security of personal data during the processing of personal data is ensured. This should include protection against unauthorized or unlawful processing, destruction and damage. Appropriate technical or organizational measures are to be taken in order to comply with this requirement, which can include data encryption or psuedonymization. This principle was included in the DPD; however, the GDPR moves this obligation under the 'data protection principles,' reinforcing the idea that data security is a fundamental obligation of all controllers and processors.

The principle of *integrity* is the property specifically of accuracy and completeness to ensure the data subjects are not jeopardized by altered, inaccurate information. The principle of *confidentiality* requires that information not be made available or be disclosed to unauthorized individuals, entities or processes. This means, personal data must be classified as confidential even within the organization, as it is extremely unlikely, that every single person in the organization needs to have access to personal data.

Relevant References: Article 32 / Recitals 74-84, 94, 95

Accountability

Article 5(2)

In addition to the six data protection principles, the GDPR introduces the principle of *accountability*, without which the others cannot be brought to life. According to this principle, the controller shall be responsible for compliance with the principles listed in Article 5(1) and must be able to demonstrate compliance, for example, documenting their decisions made when engaging processing activities.

Relevant References: Article 24

Consent

Article 7.

DPD, Article 2(h).

The data subject's *consent* shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.

GDPR, Article 4(11).

***Consent* of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.**

In an effort to facilitate proper jurisdiction, the GDPR codified a comprehensive approach for data captured and shared by obtaining, upholding and revoking consent by data subjects. Much like the previous directive, consent must be freely given, informed and revocable. The GDPR expressly states that where there is an imbalance of power between the party giving consent and the party receiving it, consent is not valid. Consent should also be evidenced by a statement or affirmative conduct to clearly indicate the purpose in context. Companies may now no longer use one statement of consent to allow data to be used in multiple ways; consent must be sought for each reason the company proposes to use the data. Consent must be active. Companies cannot rely on silence, inactivity or consent given prior to changes in policy. In addition, statements

of consent cannot be bundled with other statements such as the terms of use, or by posting a link to a company's privacy policy. The elements of valid consent have been listed as: (i) the Data Subject must have been under no pressure when consenting; ii) the Data Subject must have been duly informed about the object and consequences of consenting and iii) the scope of consent must be reasonably concrete. It must be noted that all of these requirements must be present for valid consent to exist.

Article 7(1) requires the ability to demonstrate that "the data subject has consented to the processing of his or her personal data. If consent is given in the context of a written declaration, Article7(2) states that it must be presented "in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language." This provision ensures that data subjects are aware that they are giving consent and for what particular processing of their personal data the consent is being given for. The importance of this provision is further appreciated under Article 7(3) where "the data subject shall have the right to withdraw his or her consent at any time." In light of this provision, the essence of Article 7(2) is made clear and seeks to ensure that consent is genuinely obtained to avoid processing without the necessary consent. Consent could be a written or oral statement or even electronic. Silence, pre-ticked boxes or inactivity should not therefore constitute consent.

Article 8 of the GDPR details the conditions for obtaining child consent in relation to the information society. It provides that in relation to an information society, "the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorized by the holder of parental responsibility over the child." This simply means that only Data Subjects who are above the age of 16 can provide consent to the processing of their personal data by the information society.

In an employment context, the GDPR extends individual rights to employees to object to certain processing, to have data corrected or restrict how data is used, and to be forgotten. Companies with EU employees will need to review current processes and likely look for alternative legal options for each category of personal data. The onus will be on the employer to show that the employee gave adequate consent. Employers will no longer be able to rely on generic consent clauses to data processing in employment contracts. Those clauses may fall foul of the requirement that consent be freely given, due to the imbalance of negotiating power; they are also not distinguishable from other matters. If you have offices in the EU, you will need to review your employment policies. The burden is on the employer to show that the employee gave adequate consent.

Overall, obtaining lawful consent under the GDPR will require companies to review and update current standards to ensure the systems and processes not only maintain an audit trail of consent, but also orchestrates deliberate measures when consent is withdrawn. This will apply to each and every channel through which data is captured, as well as each and every repository used to store data throughout the entire business. This presents the burden of not only the technical implementation, such as implementing an interface to edit user data, but also doing so without creating unnecessary friction in the company's day-to-day business.

DATA SUBJECT RIGHTS

Along with the expanded definition of personal data, the GDPR also provides data subjects with enhanced, powerful rights regarding how companies may retain and process their personal data. Under the current directive, data subjects hold the rights of access, rectification, erasure, objection, and the right not to be subject to automated processing decisions. The GPDR further reinforces individual rights by expanding these and introducing new ones.

Figure 5.

Existing Rights

Right Of Access Article 15.	The right of access allows individuals the ability to confirm whether or not their personal data is being processed, as well as prompt open access. Much like the directive, companies must provide categories of concern and identify any external recipients that have been or will be exposed to the data. Companies must also disclose the purpose of processing, source of, and duration for which the data will be stored under the new regulation. A key change is reflected in the timescale of response, where companies no longer have 40 days to respond but must act on the request without delay. Whereas under the directive, a nominal fee was charged for access to this information, now companies now must provide access to the consumer at no charge.
Right To Rectification Article 16.	The right to rectification provides data subjects with the ability to correct any inaccurate or incomplete information. Previously, this was only granted when necessary to ensure fair processing; however, under the GDPR, data subjects may make changes to any personal data and companies are required to share corrections with any third parties that have obtained the information.
Right To Object Processing Article 21.	The right to object processing can be sanctioned at any time by the data subject. Unlike the directive, companies now must cease objectionable processing data even if used for legitimate interests, direct marketing or even research purposes. Companies must have structures in place so that employee personal data can be easily accessed, provided upon request, and reasons behind processing can be justified.
Right To Erasure Article 17.	The right to erasure is popularly referred to as the 'right to be forgotten,' and prompts the obligation to erase personal data without delay. Under the GPDR, personal data must be removed when the data is no longer needed for the original purpose, when there are no other reasons for processing or when the individual withdraws consent. This right gained attention after a landmark case in 2014, when the ruling rejected the long-established concept of free-flowing data online. The case began in 2009, when Spanish lawyer Mario Costeja Gonzàlez requested the payment of his debt be erased by the newspaper that had published the information and for Google to expunge the links. Because his debt had been resolved many years earlier, it was no longer considered relevant by the Europe's highest court, championing a universal 'right to be forgotten.' Under the GPDR, personal data must be removed when the data is no longer needed for the original purpose, there are no other grounds for processing, or the individual withdraws consent.

New Rights

Right To Restriction Of Processing Article 18.	The *right to restriction of processing* requires companies to suspend further use while allowing existing data to continue to be stored. Similar to the 'right to erasure,' any third party linked to this data may be held liable.
Right To Data Portability Article 20.	The *right to data portability* allows individuals to obtain all records of previously-consented-to personal data held by the company and give it to an entity of their choosing, which may be a competitor. Data must be provided free of charge and without undue delay in a structured, commonly used, machine-readable format, so that the new company can readily import and make use of the data. This prospect puts power in the hands of consumers to swap to an alternate service provider using the same personal data.

ACCOUNTABILITY IN PRACTICE

Data Controller & Data Processor

Whereas liability once waived the distinction between 'data controllers' and 'data processors,' the GDPR applies directly to both roles. The data controller is the entity determining the purposes for which, and the way in which, personal data is processed. By contrast, the data processor is any entity directly involved in collecting, storing and transferring personal data. Sometimes the controller and processor are the same entity; sometimes one is using the services of the other; yet, both must adhere to the GDPR. To fall under the scope of regulation, the GDPR implicitly states that it is not necessary to directly collect, store or destroy the data, and it is sufficient to retrieve, consult, organize, structure, align, combine, disseminate, disclose by transmission or soft-delete data about EU individuals. In other words, the GDPR impacts every entity handling or using the data of an EU data subject—in essence, every professional in the modern era business.

Records Of Processing Activities

Article 30.

The GDPR represents a paradigm shift for companies. Under the 1995 EU Directive currently in force, companies are expected to give notice to competent data protection authorities prior to engaging in certain processing activities.

The GDPR removes prior-notice obligations and instead requires controllers to maintain records of all processing activities, including for certain, specified types of information. The purpose of these records is to allow the controller to demonstrate compliance with GDPR requirements, and records must be made available to the relevant supervisory authority upon request. To comply with this obligation, companies must begin conducting data protection audits to make an inventory of the different personal data processing activities carried out within an organization. Companies that do not begin to implement recordkeeping as the effective date of the GDPR approaches will certainly face difficulties in complying with the GDPR's requirements.

Under the GDPR, both controllers and processers must demonstrate compliance accountability as an enumerated legal requirement. This will require both entities to implement a compliance framework to demonstrate activities in accordance, rather than merely confirming as such. As such, the regulation infers obligations to keep detailed records on how information is used and stored, as well as documenting decisions made outside of the processes in place.

Controller

Article 30(1)

(a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;
(b) the purposes of the processing;
(c) a description of the categories of data subjects and of the categories of personal data;
(d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organizations; where applicable, transfers of personal data to a third country or an international organization, including the identification of that third country or international organization and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of appropriate safeguards;
(f) where possible, the envisaged time limits for erasure of the different categories of data;
(g) where possible, a general description of the technical and organizational security measures referred to in Article 32(1).

Processor

Article 30(2)

(a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;
(b) the categories of processing carried out on behalf of each controller;
(c) where applicable, transfers of personal data to a third country or an international organization, including the identification of that third country or international organization and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of appropriate safeguards;
(d) where possible, a general description of the technical and organizational security measures referred to in Article 32(1).

Data Protection By Design And By Default

Article 25.

The GDPR requires companies to implement measures to ensure an appropriate level of security is in place for processing. This is embraced and codified through the concept that requires data privacy as a default to business operations. Rather than considering how to incorporate privacy after a new product or strategy has been designed, companies will be expected to embed data privacy into all business processes and functionalities from the outset. This will also require entities to: (i) minimize data collected, (ii) not retain that data beyond its original purpose and (iii) give the data subject access and ownership of that data. Recital 78 provides controllers with measures that should be adopted to meet the principles of data protection by design and data protection by default.

Recital 78

Such measures could consist inter alia, of minimizing the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features.

Traditionally, anonymous data has not been subject to data protection laws. However, in today's digital world, anonymized data can easily link to revealing one's identity and it is not very hard to build a profile of a person without the traditional means of identification such as a name or address. For example, a team at Harvard was able to identify individuals from anonymized data in a genetics database by cross-referencing it with other public databases.[35] The accuracy rate was 42 percent based on the use of only three types of information—zip code, date of birth, and gender—rose to 97 percent when the first name was added. Another example came from a team of researchers at the University of Texas at Austin who used de-anonymization tools on 500,000 Netflix users who had "anonymously voted" for their preferred movies back in 2007.[36] In this case, the researchers were also able to identify users by linking votes with another public database with movie ratings. Both of these studies illustrate that the use of anonymous data may constitute an intrusion of an individual's privacy.

Unlike the current directive, the GDPR introduces the concept of 'pseudonymizing.' Much like anonymization, *pseudonymization* is a process of replacing identifiable attributes with values to prevent the individual from being directly identified. The key difference between the two, is keeping the identifiable attributes inaccessible to users of "pseudonymized data." Simply put, 'pseudonymization' is a method to substitute identifiable data with a reversible, consistent value. *Anonymization* is the destruction of the identifiable data, liable to indirect re-identification. After 'pseudonymizing,' data is no longer directly identifiable, but can still be referred back to a specific individual when combined with other data and statistical analysis.

The rise of pseudonymization can be seen as a response to technicalogial advances. By introducing the new concept, the GDPR acknowledges that even seemingly impersonal data can be personally identifying, but that such data is potentially valuable. Because 'pseudonymizing' data reduces the privacy risks for data subjects, the GDPR's requirements are relaxed (though not altogether removed) when companies use this process for personal data that they collect; the upcoming regulation seems to accept that data will be reused more frequently for novel purposes, and offers guidance to that end. By designating formal avenues for the use of data, the GDPR is in essence, accepting the value of data, so long as it is used in a lawful way. Recital 78 also refers to the 'Data Minimization Principle,' in which the minimum required is collected and processed for the expressed intended use. Recital 83 advises controllers to evaluate the risks of processing and implement measures to mitigate those risks, such as encryption and ensuring an appropriate level of security, including confidentiality.

Recital 83

In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as encryption. Those measures should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected. In assessing data security risk, consideration should be given to the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage.

Data Protection Officer

Articles 37-39.

The GDPR requires Data Protection Officers (DPO) to be appointed for all public authorities, and where core activities involve "regular and systematic monitoring of data subjects on a large scale" or where the entity conducts large-scale processing of "special categories of personal data." Though an early draft of the GDPR limited mandatory DPO appointment to companies with more than 250 employees, the final version has no such restriction.

The regulation does not define the specific credentials DPOs must carry; however, where required, the DPO should be aptly appointed "on the basis of professional qualities, including "expert knowledge of data protection law and practices." Guidelines under Article 29 from the EU Working Party (WP29) were later published to better interpret language within the regulation, which states that required levels of expertise "must be commensurate with the sensitivity, complexity and amount of data an organization processes. The DPO should thus be chosen carefully, with due regard to the data protection issues that arise within the organization."[37] In Oxford University's International Data Privacy Law journal, Eric

Lachaud reached the conclusion that the most appropriate certification for the DPO is a combination of the IAPP's Certified Information Privacy Professional credential for EU professionals (CIPP/E) and Certified Information Privacy Manager (CIPM).[38] The IAPP also offers the Certified Information Privacy Technologist (CIPT) credential, as well as a version of the CIPP for the U.S. The DPO is not an at-will position and must inherit protected employment status under a four-year term. The DPO is not required to work solely for a single entity and may be appointed to a group of undertakings, provided the part is easily accessible for all.

DPO positions are expected to be highly competitive and sought after. In fact, an International Association of Privacy Professionals (IAPP) study reported that the upcoming EU regulation will create a demand for "at least 75,000" DPOs worldwide.

The study, which was designed to determine the global reach of the GDPR, found that the U.S. will have the largest demand for DPOs (9,000), followed by China (7,568), Switzerland (3,103) and Russia (3,068).

The Case For A DPO At Every Company

Data Protection Officers assume a vital and powerful role for both controllers and processors, and while this mandate is not required for many within the industry, EU regulators highly encourages a DPO designation. The concept of a DPO or a DPO-like position has considerable merit for any company concerned about data security. The GDPR envisions the DPO as the internal executive authority on data privacy legalities and enforcement. This role embodies expert knowledge and their core activity is to stay up to date with all relevant compliance requirements, not only those defined in GDPR, but country- and industry- specific regulations. Creating a DPO-like position is not just a matter of internal self-defense, it's a proactive, strategic move that offers significant opportunities.

What Now?

THE GDPR IMPACT

Enforcement

EU-member Supervisory Authorities (SAs) will be responsible for enforcing the upcoming GDPR through investigative and corrective powers, including directly against U.S. companies that have a physical presence in the EU. U.S. companies without a physical presence in the EU but that knowingly and actively conduct business in the EU are required to designate a representative located in the EU. In this vein, each representative is prompted the discretionary ability to determine if a U.S. company was purposely collecting EU resident data and enforce breach.

Complaints may be received not only from the Data Subjects themselves but also from any organization or association that either chooses to make a complaint or has been chosen by a data subject to represent their interests. These complaints can be submitted to any Supervisory Authority, not just the SA holding territorial responsibility. In contrast with the previous Directive, the GDPR grants SAs a broader scope of responsibilities and sovereignty including investigative, corrective and authoritative powers.

Investigative powers allow SAs the ability to undertake any complaint received and employ a wide range of measures, including audits or open access to company assets. Corrective powers include the ability to issue warnings, reprimands and orders to bring processing operations into compliance. SAs also hold the right to impose temporary or definitive bans, withdraw certifications, order breaches to be communicated to data subjects, cease data flows altogether and even levy substantial fines.

Penalties

Fines

Under the existing Directive, penalties are determined by national law and the maximum is generally low (e.g. in the UK, the largest single fine issued to date is £400,000 or nearly $535,000).[39] Along with the strengthened policies, the GDPR codifies a penalty structure for violations. Failure to comply

with the requirements could result in financial penalties up to €20 million (approximately $23.5 million) or four percent of a company's global annual revenue, whichever is higher. With the assistance of U.S. authorities, EU regulators can also fine U.S. companies for violating the GDPR.

Breach Notification

Because privacy is such a high priority in the new regulation, the GDPR also includes a new breach notification rule. The inclusion of this rule not only highlights the importance of data privacy, but also holds entities accountable for security failures. In the case of a privacy breach, the GDPR requires companies to report the incident to SAs within 72 hours of the discovery of becoming aware.

It is no secret that data breaches are common. In November 2017, Risk Based Security indicated 3,833 reported data security breaches globally, exposing nearly over seven billion personal records. The number of records exposed due to data breaches in the first nine months of 2017 is up 305 percent compared to 2016.[40]

NEXT STEPS

In an effort to transform data protection culture as well as practice, the GDPR has bold ambitions, and its impact will likely be profound. It advocates for data protection to exist at the core of business values, instead of a casual afterthought. For most U.S.-based companies, the regulation's requirements may be uncontroversial and appear as suggested 'best practices,' at best.

And while the direct impact may seem far-flung for many, the potential ramifications fuel much of modern-day corporate strategy. In fact, a recent survey by PricewaterCoopers revealed the GDPR as a top priority for 92 percent of U.S. companies.[41] Given the stringent list of requirements of the regulation, there are three possible scenarios for companies to adopt: **ignore it, avoid it, embrace it**.

– Ignore It –

The advent of technology has transformed the traditional forms of communication, connection, including the face and the pace of business. As a catalyst to new infrastructures, new monopolies, new politics and new economics, technology is changing who is participating, how business is done across borders, how rapidly competition moves and where the economic benefits are going and not going. The near-zero marginal costs of digital communications and transactions open new possibilities for conducting business on a massive scale. Data once collected manually and stored in drawers is now systematically mechanical and stored in a cloud.

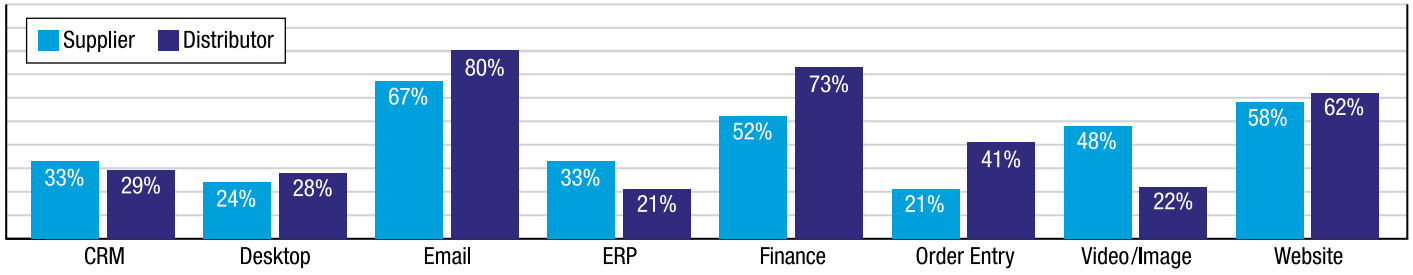
The cloud dates back to 1997, when Emory University Professor Ramnath Chellapa defined the new "computing paradigm where the boundaries of computing will be determined by economic rationale rather than technical limits alone."[42] This has become the heart of what the cloud has evolved to today. In 1999, Salesforce.com became the first major driver of the cloud. In their earliest form, cloud services were promoted as delivering enterprise-level IT resources anytime, anywhere. Historically, telecommunication companies offered single, dedicated point-to-point data connections and involved building out physical infrastructure to allow more users to have their own connections. The newly designed cloud network not only allowed shared access to more users, but it could be enabled at a fraction of the cost. Since then, the cloud has grown into a powerful tool for businesses to monitor and analyze every interaction, create a unified repository of information and generate actionable intelligence in real time.

Cloud computing has fueled digital transformation like no other technology disruption before it. Not only has it changed how companies of all sizes and business sectors consume technology, but it continues to innovate at breakneck speed. Cloud platforms enabled new, complex business models and orchestrated more globally-based integration networks in 2017 than many analysts had projected. Thanks to an increasing rate of adoption among SMEs, leading researchers, including Forrester, are adjusting their forecasts upward. Forrester's 2018 predictions expect cloud computing to accelerate enterprise transformation everywhere.[43] The November 2017 predictions reflect the growing dominance of cloud application and development platforms and their role in revolutionizing new business models across enterprises today. In fact, nine in 10 business leaders believe cloud computing is the future of modern enterprise, according to the results of Evolve IP's 2017 North American Cloud Adoption Survey.[44] Some of the most popular reasons for the growing dominance in using the cloud are flexibility, scalability and reliability. The Cloud Industry Forum (CIF) study also cited 'innovation support' as an emerging key driver for investment in the cloud.[45]

The cloud was originally and rightly seen under the domain of the IT department, but today it serves a multitude of functions used by different business units. Beyond internal infrastructure, changing technology is forcing disruption and innovation in ways businesses reach their customers.

And that's no exception to the promotional products industry. According to the 2015 PPAI Technology Study, 31 percent of distributor companies and 41 percent of supplier companies, on average use cloud hosting providers (Figure 6). The large majority believe cloud services have made business easier and 53 percent of suppliers, as well as 39 percent of distributors plan on investing more in cloud services. Whereas 29 percent of small distributors reported the plan to strengthen cloud capabilities, that number nearly triples when querying large distributors, 81 percent of which indicated plans to increase investments.

Figure 6. Cloud Services Used By Promotional Products Industry



Source: 2015 Technology Study (PPAI Research, December 2015)

The rapidly growing use of cloud services, the disappearing perimeter between internal and external networks and an influx of new devices are challenging traditional methods of protecting sensitive data, as well as giving rise to security problems. Data can no longer be physically protected; ironically, it is the rapid growth of challenges that is fueling the expansion of the threat landscape. The increase in connected objects and the amount of data generated have created a valuable asset for businesses as well as cybercriminals. Each connection creates a new attack vector for a hacker to target, infiltrate and take control. And the risks will understandably increase as connected objects proliferate.

Unsecured wireless devices and even cloud architecture have come under attack in recent years. Malware is a malicious type of software code that plays a significant role in data security breaches. The 2017 Global State of Information Security® Survey by PricewaterhouseCoopers, logged 38 percent of attacks as malware, a malicious type of software code that plays a significant role in data security breaches.[46] Malware is typically deployed through a phishing email message scam. This involves an unsuspecting victim receiving an email message from a fraudulent source, a victim clicks on a nefarious link or opens an attachment of the email that contains the malware. Ransomware is set to be the most influential virus of 2017.[47] This growing threat generally involves a virus that is discrete, yet powerful. Unlike other malware business models, in which sensitive data is stolen and sold on the darknet, hackers who utilize ransomware as their attack vector receive payment directly from their victims. They do so by disrupting the victim's environment, and their reward is made possible by the anonymity provided by digital currencies such as bitcoin.

According to research by professional services company Accenture, only one percent of cloud services provide notification of security incidents in fewer than 24 hours and 84 percent of cloud services do not immediately delete customer data on termination of contract.[48] In a joint-study with independent research firm Ponemon Institute and Accenture, IBM reported the average cost of cyber-crime globally climbed to $11.7 million per organization in 2017 and companies in the United States incurred the highest total average cost per crime at $21.22 million. The next highest average was found in Germany at USD $11.15 million.

IBM Chairman, CEO and President Ginni Rometty recently said that cybercrime may be the greatest threat to every company in the world.[49] Nobody is immune; almost all companies, private and public, large and small, use common software, hardware and cloud services. Shamini Peter, Chief Operations Officer for promotional products distributor Axis Promotions, says she believes every company in the promotional products industry will see some form of impact from the regulation.

The rise in cybercrime and associated costs makes ignoring the GDPR a challenging task. Cyberinsurance policies will likely begin to mimic the GDPR language. Thus, a violation of GDPR rules may result in a denial of coverage.

> **"Every company in the promotional products industry will see some form of impact."**
> **— Shamini Peter, COO of Axis Promotions**

– Avoid It –

A year into his tenure as CEO of Google, Sundar Pichai declared his vision of the future at an October 2017 'Made By Google' product announcement: AI.[50] Pichai questions how to apply artificial intelligence to rethink every product; he doesn't want to make AI just another feature, but fundamentally ingrain every object in our lives.

Pichai's vision not only presents the evolution of products into intelligent, connected devices, but particularly provides a glimpse into the future of the promotional products industry. As an industry defined by the future of product, 'data-enabled' may be the default for every object in the marketplace. Soon, traditional sources of data will soon be supplemented by another source—the product itself. Smart, connected products will generate real-time information, unprecedented in its complexity and sheer volume. These new types of products will alter the structure of the industry, exposing companies to new competitive opportunities and threats. For example, data about the product's functionality could be valuable to suppliers of those components, and its performance and usage could ultimately provide end-buyers with the direct ROI.

However, all this data opens up new vulnerabilities to private and sensitive information and brings on new challenges of securing it, governing it and protecting privacy. Much like the constraints imposed by the GDPR, in choosing how to capture new value from product data, companies must also consider the how to securely manage data security. In its most recent report, "Data Age 2025," the International Data Corporation (IDC) pinpoints a significant gap between the amount of data being produced today that requires security and the amount of data that is actually being secured, and expects this gap to widen. In fact, IDC predicts that by 2025, almost 90 percent of all data created in the global datasphere will require some level of security, but less than half will be secured.[51]

At its core, smart and connected products are controlled by their users. And while some users may not care how their data is used, others may feel strongly about the privacy and exploitation of it. Companies that choose to ignore the data protection requirements may put themselves at risk of a disrupting the customer experience and potentially damaging a company's reputation. A staggering majority of Americans are concerned about businesses collecting and using personal information, and 95 percent of consumers are more loyal to brands that protect their data's privacy, according to a recent a survey conducted by TechValidate.[52]

While regulatory in nature, GDPR should elevate core values of trust and of building relationships that will enable companies to build on data and gain more value in the marketplace. Failure to implement successful, compliant data protection measures may damage a company's reputation, customer relationships and, ultimately, its financial security. No matter how minimal of a footprint, every U.S. company should get well acquainted with the demands of GDPR. Simple ignorance garners the potential to be on the wrong end of a GDPR request, and the odds are stacked against one's favor. In fact, research and advisory company Gartner predicts that by the end of 2018, fewer than 50 percent of companies affected by the GDPR will be in full compliance with its requirements.[53]

Creating trust online is a fundamental challenge to ensuring that the opportunities emerging in the information economy can be fully leveraged. The handling of data is a central component in this context. In today's digital world, personal data are the fuel that drives much commercial activity online. However, how this data is used has raised concerns regarding privacy and the security of information. As the global economy shifts further into a connected information space, the relevance of data protection and the need for controlling privacy will further increase. Understanding different approaches to and potential avenues for establishing more compatible legal frameworks at national, regional and multilateral levels is important for facilitating international trade and online commerce. The rules surrounding data protection and cross-border flows of data affect individuals, businesses and governments alike, making it essential to find approaches that address the concerns of all stakeholders in a balanced manner.

By 2025, almost 90 percent of all data created in the global datasphere will require some level of security, but less than half will be secured.

Today's websites and apps are powered by sophisticated technology. In order to meet increasing consumer expectations for search capabilities, content consumption, deliverables and more, websites must incorporate robust solutions on the backend. The promotional products industry alone has seen a 55 percent increase in 'online sales' over 10 years, according to the recent *PPAI Sales Volume Study* (Figure 7, page 23). The study defines *online sales* as reflecting any promotional product revenue initiated online, but does not include any merchant-aided transactions fulfilled online.

Therefore, online sales could be generated from a range of sources including desktop browsers, applications and mobile devices. Not surprisingly, 65 percent of distributors have mobile-friendly websites, as indicated in the 2015 PPAI *Technology Study*. Given the broad online footprint of the industry, companies that ignore the GDPR do so at their own peril.

To put it bluntly: you can't control what you don't see. Digital properties have more third-party code than most realize and this code is compromised more often than you think. A new study conducted by the RiskIQ Threat Research team reveals that some major U.S. firms still have websites that don't comply with the GDPR. RiskIQ discovered that 68 percent had significant security gaps in PII collection and each organization identified an average of 1,891 insecure login forms, 1,663 pages collecting PII insecurely, 1,326 EU first-party cookie violations and 1,265 EU third-party cookie violations.[54]

Figure 7.

Promotional Products Industry Sales

	2006	2011	2016	10 Year Growth
Industry Total Net-Worth*	$18.1B	$17.7B	$21.3B	▲18%
Offline Sales	$15.4B	$14.6B	$17.1B	▲11%
Online Sales	$2.7B	$3.1B	$4.2B	▲55%

**The promotional products industry total net worth is based on actual sales reported by U.S. promotional consultant companies in the PPAI annual* Sales Volume Study *report. The figures represent an estimate on the promotional sales of U.S. distributors, including both PPAI members and nonmembers. Figures project across the entire distributor population combined sales for small distributors (under $2.5 million) and large distributor firms (over $2.5 million).*

Source: 2016 Sales Volume Study (PPAI Research, July 2017)

Chris Olson, the CEO and co-founder of software company The Media Trust, says that up to 75 percent of the code executing on a typical website belongs to more than 300 outside vendors. Most brands, he said, "don't track what code these outside vendors have placed on their sites and often don't even know the vendors' names." The startup found that even the simplest websites average 10 third-party vendors. These vendors continuously change and so do their actions. Olson believes that the GDPR's impending arrival means "it's no longer feasible for website operations teams to have an incomplete picture of their digital ecosystem."[55]

The upcoming regulation poses dozens of new obligations and technical requirements that present pitfalls for companies should they fail to alter their established business practices, regardless of existing processes and procedures already in place. Companies with a public website, social media accounts or email servers, regardless of whether a transaction occurs, may be subject to the GDPR.

– Embrace It –

The promise and peril of data is inevitable. Much like the evolving regulatory landscape, change is pervasive and continuous.

With an expanding risk universe, supply chains can be disrupted by new technologies, unsuspected cyber-crime and the continuous evolving regulatory landscape, and other uncontrollable events. The GDPR enters into force at a crucial time for the digital economy and ecosystem; one in which substantial risks to rights and liberties are emerging, while at the same time vast opportunities to create value, promote welfare and enhance objectives are unfolding.

The availability of and access to data, along with the advanced tools to make sense of the numbers, offers a new way of understanding in the world. The advent of technology has transformed the traditional forms of communication, connection, including the face and the pace of business. As a catalyst to new infrastructures, new monopolies, new politics and new economics, technology is changing who is participating, how business is done across borders, how rapidly competition moves and where the economic benefits are going and not going. And yet, the future of the industry is not shaped by the future of product. In fact, Vice Chairman of Ogilvy & Mather, Rory Sutherland, said "the next revolution will be psychological, not technological."[56]

Many equate the digital economy with the Information Technology (IT) sector; however, the IT sector falls short in measuring the complete scope because, as McKinsey notes, "digitization, like electricity, is a general-purpose technology that underpins a huge share of economic activity far beyond the sector that supplies it."[57] This will be an era not of man versus machine, but man collaborating with machine. In addition to technological change, this new age requires us to change how we do our work.

What also must be recognized is that GDPR is an evolution in data protection, not a total revolution. It demands accountability from companies for their use of personal data, and it enhances the existing rights of individuals. Innovation in the future won't be about continually making new iterations of products but about finding new ways to make people value and want the products. A better understanding of what people value, how they behave and how they make choices could generate just as much economic value. An insights-driven business systematically harnesses data and applies analytically-derived insight to create a competitive advantage. A recent report by Forrester forecasts insights-driven companies will grow 27 percent and startups 40 percent annually, eight times faster than global GDP, projected at 3.5 percent.[58]

Conclusion

COMPLIANCE CHECKLIST

The GDPR enters into force at a crucial time for the digital economy and ecosystem; one in which substantial risks to rights and liberties are emerging, while at the same time vast opportunities to create value, promote welfare and enhance objectives are unfolding. There is a massive opportunity for data to effect positive change on all of human society. Not only is data making business more effective, but it is in the process of transforming every aspect of the individual's life. Data alone doesn't create competitive advantage; competitive advantage becomes a reality when companies analyze and act on the data. Data without rigorous analysis is at best just rhetoric and, at worse, incredibly harmful. In order to be successful beyond the requirements of the GDPR, companies must also consider related **people** and **processes** during preparation and implementation.

People

People are key to implementing a company's data privacy rulebook. The GDPR isn't a regulation that holds a single individual accountable, but one that could hold a company accountable for a single individual's actions. Saying 'I wasn't aware' is not going to be a valid excuse if audited. Because of this, it becomes incumbent in instilling a culture of awareness running in parallel across multiple business lines and geographies. Culture can be defined as "an integrated pattern of human knowledge, belief and behavior," one that "characterizes an organization."[59] Privacy should be closely aligned with the company's value system, and proper training should help embed behaviors that will shape the culture over time.

Training is also essential to embedding a privacy program and building a corporate privacy culture. Staff need to know the baseline legal requirements in the organization's approach, and why the organization thinks data protection is important. Data privacy should be top of mind for every employee and should engender a greater sense of responsibility and accountability. Training can create awareness of how employees should take notes and record information about customers, prospects, and employees, as well as how to follow online security protocols such as how to recognize phishing emails and the dangers of clicking on unrecognized email attachments.

Process

Given the increasing complexity of the cyberworld, companies should no longer rely solely on ad hoc privacy processes. Even then, awareness and proper training won't single-handedly eliminate every threat, detect every breach or resolve every problem. Data protection is now everyone's job and that will call for a high-grade, cross-functional plan.

The GDPR will concern every channel through which data is collected, including website, email or POS systems, as well as the repositories used to store data, including CRMs, cloud hosting providers and internal infrastructure. Each data point will need thorough monitoring to document where it is coming from, what it is being used for, where and how is it being stored, who is responsible for it, and who has access to it.

START NOW

No company that operates on a global footprint, whether directly or through an array of third parties, can afford to ignore or avoid preparation for the GDPR. For most, this is a critical time to reevaluate the people and processes related to data protection and build flexible solutions to meet today's challenges to continue tomorrow's growth. By engaging the people who deal with these processes in a conversation about the GDPR and why it is important, companies will be better equipped to update processes with the necessary requirements to become GDPR compliant.

While no business can possibly second-guess what future regulations will mandate, a simple analogy helps: much like flows of dollar, where each business unit manager and executive can account for every dollar coming in and going out, the long-term outlook will be to gain fluency in reading digital data ledgers as they are income statements.

The bottom line is that the EU has set a new standard in data protection, and companies that embrace these new standards will be well prepared for the coming shift in expectations.

Appendix

RESOURCES

Full text of the GDPR available in the Official Journal of the European Union

The European Union: A Guide For Americans

THE EUROPEAN UNION

There are currently 28 countries that represent the European Union (EU) as 'member states.' The EU population is estimated at 511.8 million[60] compared to 326.2 million in the United States.[61]

Twenty-two member states participate in the 'Schengen Area' of free movement in which internal border controls have been removed, eradicating the need for passports. Bulgaria, Croatia, Cyprus, Ireland, Romania and the United Kingdom are currently not affiliated with the Schengen Area; however, Bulgaria and Romania are currently in the process of joining. There are also non-EU States within the Area including Iceland, Norway, Switzerland and Liechtenstein.[62]

Figure 8. Members Of The European Union (EU)

Member States (shaded dark blue)

Austria (AT)	Luxembourg (LU)
Estonia (EE)	Slovenia (SI)
Italy (IT)	Cyprus (CY)
Portugal (PT)	Greece (EL)
Belgium (BE)	Malta (MT)
Finland (FI)	Spain (ES)
Latvia (LV)	Czech Republic (CZ)
Romania (RO)	Hungary (HU)
Bulgaria (BG)	Netherlands (NL)
France (FR)	Sweden (SE)
Lithuania (LT)	Denmark (DK)
Slovakia (SK)	Ireland (IE)
Croatia (HR)	Poland (PL)
Germany (DE)	United Kingdom (UK)**

Candidate Countries

Albania (AL)	Serbia (RS)
Montenegro (ME)	Turkey (TR)
Republic of Macedonia (MK)***	

Potential Candidates

Bosnia & Herzegovina (BA)
Kosovo (XX)****

*as of November 2017
**in March 2017, British Prime Minister, Theresa May formally notified the European Council of the United Kingdom's decision to leave the EU. Legally known as Article 50, the UK's announcement initiated the formal withdrawal process, estimated to take up to two years. The UK remains a full member of the EU until it completes withdrawal negotiations, a process that has not yet begun.
***formerly Yugoslav
****under UNSCR1244

Source: europa.eu

EU Institutions

Each of the countries within the EU are independent, yet work through three main governing bodies, which include the European Commission, Council of the European Union and the European Parliament. EU member states have "pooled sovereignty," in which decision-making powers are delegated to its respective governing body, referred as the European Institutions, depending on the subject under consideration.[63]

Commission

In its executive capacity, the Commission acts as the 'government' in a parliamentary system by initiating legislation and submitting proposals to the Council of the European Union. The Commission also oversees Member States' implementation of directives, and enforces regulations.
Official Website: ec.europa.eu/commission/index_en

European Council

The European Council (EC) is the EU institution that defines the general political direction and priorities of the European Union.
Official Website: www.european-council.europa.eu/en

European Parliament

The European Parliament (EP) is composed of representatives directly elected by the people of the Member States. In most cases the EC is required to submit proposed legislation to the Parliament for comment. The EP acts as a forum for debate and questioning of the Council and Commission. The Parliament adopts EU, exercises democratic control over the Commission, and owns joint authority with the Council to approve the EU budget.
Official Website: www.europarl.europa.eu/portal/en

Court of Justice

The European Court of Justice (ECJ) is the judicial institution of the EU and highest legal authority. The EJC ensures that EU treaties are interpreted and applied in the same way in every Member State. It is located in Luxembourg and is comprised of 28 judges, one from each Member State. In addition to the 28 judges at the ECJ, there are 8 Advocate Generals who provide opinions on cases to assist the ECJ in making its decisions.
Official Website: curia.europa.eu/jcms/jcms/j_6/

EU Currency

The Euro was launched the beginning of January 1999 with a single exchange rate and monetary policy run by the European Central Bank (ECB). To-date, 19 EU member states use the common currency, comprising what's known as the 'Eurozone.' The countries in the Eurozone as of 2017 are: Austria, Belgium, Cyprus, Estonia, Finland, France, Germany, Greece, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, The Netherlands, Portugal, Slovakia, Slovenia and Spain.[64] Internationally, the Euro gives the EU "more clout, as it is the second most important international currency after the U.S. dollar."[65]

Non-Euro Area

Bulgaria - Lev (лв)
Croatia - Kuna (kn)
Czech Republic - Koruna (Kč)
Hungary - Forint (Ft)
Poland - Złoty (zł)
Romania - Leu (lei)*
Sweden - Krona (kr)

Countries With Opt-Out

Denmark, Faroe Islands, Greenland - Krone (kr)
United Kingdom, Northern Ireland, Scotland - Pound (£)

EU Languages

Bulgarian, Finnish, Italian, Romanian, Croatian, French, Lithuanian, Slovak, Czech, German, Latvian, Slovenian, Danish, Greek, Maltese, Spanish, Dutch, Hungarian, Polish, Swedish, Estonian, Irish, Portuguese

EU Website Domains

.de .eu
.fr .ie

**Romania has committed to the Euro once it fulfills the necessary conditions*

REFERENCES

1 Jan Philipp Albrecht, "How The GDPR Will Change The World" European Data Protection Law Review, Volume 2, Issue 3. (March 2016) 287-289. edpl.lexxion.eu/data/article/10073/pdf/edpl_2016_03-005.pdf.
2 Samuel D. Warren, Louis D. Brandeis. "The Right To Privacy." Harvard Law Review, Volume 4, Number 5 (December 1890).193-220. www.jstor.org/stable/1321160.
3 Serge Gutwirth. Privacy And The Information Age. Oxford: Rowman & Littlefield Publishers, Inc. (2002).
4 Farhad Manjoo. "The Online Ad Industry Is Undergoing Self-Reflection. That's Good News" The New York Times (April 2017) www.nytimes.com/2017/04/05/technology/online-ad-industry-self-reflection.html.
5 Jennifer Rankin. "Facebook Fined £94M For 'Misleading' EU Over WhatsApp Takeover" The Guardian (May 2017). www.theguardian.com/business/2017/may/18/facebook-fined-eu-whatsapp-european-commission.
6 Dan Solove. The Digital Person: Technology And Privacy In The Information Age (New York University Press, 2004), 43.
7 European Commission "Commission Proposes A Comprehensive Reform Of Data Protection Rules To Increase Users' Control Of Their Data And To Cut Costs For Businesses" Press Release (Brussels, January 2012). europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en
8 "Consolidated Version Of The Treaty On European Union" Official Journal Of The European Union. (October 2012). eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0023.02/DOC_1&format=PDF
9 Official Website Of The European Union, October 2017. europa.eu/european-union/index_en
10 www.nobelprize.org/nobel_prizes/peace/laureates/2012
11 Isabelle Ioannides, "Rule Of Law In European Union External Action: Guiding Principles, Practices And Lessons Learned" International Institute For Democracy And Electoral Assistance (Strömsborg, 2014).
12 Rafał MAŃKO. "The EU As A Community Of Law: Overview Of The Role Of Law In The Union" Briefing (European Parliament Think Tank, March 2017), 12. www.europarl.europa.eu/RegData/etudes/BRIE/2017/599364/EPRS_BRI(2017)599364_EN.pdf
13 "EU Law" Official Website Of The European Union. europa.eu/european-union/law_en
14 "Convention For The Protection Of Individuals With Regard To Automatic Processing Of Personal Data." European Treaty Series No 108. (Council Of Europe, Strasbourg: January 1981) www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108.
15 "Article 288" Consolidated Version Of The Treaty On The Functioning Of The European Union, Official Journal Of The European Union. eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E288
16 Jiahong Chen, "How The Best-Laid Plans Go Awry: The (Unsolved) Issues Of Applicable Law In The General Data Protection Regulation" International Data Privacy Law, Volume 6, Issue 4. (November 2016), 310. doi.org/10.1093/idpl/ipw020.
17 "Sources And Scope Of European Union Law" European Parliament. www.europarl.europa.eu/atyourservice/en/displayFtu.html?ftuId=FTU_1.2.1.html
18 "LIBE Committee Vote Backs New EU Data Protection Rules." European Commission Press Release Database (October 2013). europa.eu/rapid/press-release_MEMO-13-923_en.htm.
19 "2.2(b) Recitals" 2011 Interinstitutional Style Guide. (Publications Office Of The European Union, Brussels: 2011). publications.europa.eu/code/en/en-120200.htm.
20 Directive 95/46/EC. edps.europa.eu/sites/edp/files/publication/dir_1995_46_en.pdf
21 Article 29 Data Protection Working Party "Statement On The 2016 Action Plan For The Implementation Of The General Data Protection Regulation (GDPR)" 442/16/EN, WP 236 (February 2016). ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp236_en.pdf
22 "Adoption Of 2017 GDPR Action Plan" Press Release (Brussels, January 2017). ec.europa.eu/newsroom/document.cfm?doc_id=41387
23 Article 29 Working Party. "Guidelines on the right to data portability" WP 242 rev.01 (December 2016). ec.europa.eu/newsroom/document.cfm?doc_id=44099
24 Article 29 Working Party. "Guidelines on Data Protection Officers ('DPOs')" WP 243 (December 2016). ec.europa.eu/newsroom/document.cfm?doc_id=43823
25 Article 29 Working Party. "Guidelines for identifying a controller or processor's lead supervisory authority" WP 244 rev.01 (December 2016). ec.europa.eu/newsroom/document.cfm?doc_id=44102
26 Article 29 Working Party. "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679" WP 248 rev.01 (April 2017). ec.europa.eu/newsroom/document.cfm?doc_id=44102
27 Article 29 Working Party. "Guidelines on Personal data breach notification under Regulation 2016/679" WP 250 (October 2017). ec.europa.eu/newsroom/document.cfm?doc_id=47741
28 Article 29 Working Party. "Guidelines on Consent under Regulation 2016/679" WP 259 (November 2017). ec.europa.eu/newsroom/just/document.cfm?doc_id=48849
29 Article 29 Working Party. "Guidelines on transparency under Regulation 2016/679" WP 260 (December 2017). ec.europa.eu/newsroom/just/document.cfm?doc_id=48850
30 Article 29 Working Party. "Opinion 2/2017 on data processing at work" WP 249 (June 2017). ec.europa.eu/newsroom/document.cfm?doc_id=45631
31 "On The Protection Of individuals In Relation To The processing Of Personal Data In The community And Information Security." Commission Of The European Community COM(90), 314 (Brussels, September 1990). aei.pitt.edu/3768/1/3768.pdf.
32 Article 29 Working Party. "Opinion 4/2007 On The Concept Of Personal Data" WP 136 (June 2012). ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf
33 Lee A. Bygrave. "Digital Rights Management and Privacy – Legal Aspects in the European Union." in Eberhard Becker, et al (Eds), Digital Rights Management. (June 2003). 426.
34 Erika McCallister, Tim Grance, Karen Scarfone. "Guide To Protecting The Confidentiality Of Personally Identifiable Information (PII): Recommendations Of The National Institute Of Standards And Technology (NIST)" Special Publication 800-122 (U.S. Department Of Commerce, April 2010). nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf
35 Latanya Sweeney, Akua Abu, Julia Winn. "Identifying Participants In The Personal Genome Project By Name." White Paper 1021-1 (Harvard University: Data Privacy Lab, April 2013). dataprivacylab.org/projects/pgp.
36 Arvind Narayanan, Vitaly Shmatikov. "Robust De-Anonymization Of Large Datasets: How To Break Anonymity Of The Netflix Prize Dataset" (UT Austin, February 2008). arxiv.org/PS_cache/cs/pdf/0610/0610105v2.pdf
37 Data Protection Working Party 29, 16/EN WP 243 "Guidelines On Data Protection Officers ('DPOs')" (December 2016). ec.europa.eu/newsroom/document.cfm?doc_id=43823
38 Eric Lachaud. "Should The DPO Be Certified?" International Data Privacy Law, Volume 4, Issue 3. (August 2014), 189-202. doi.org/10.1093/idpl/ipu008.
39 "TalkTalk Gets Record £400,000 Fine For Failing to Prevent October 2015 Attack" Information Commisioner's Office (October 2016). ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2016/10/talktalk-gets-record-400-000-fine-for-failing-to-prevent-october-2015-attack.
40 "Data Breach Trends: First Nine Months Of 2017" Data Breach QuickView Report. (Risk Based Security, November 2017).
41 "Pulse Survey: US Companies Ramping Up General Data Protection Regulation (GDPR) Budgets" GDPR Preparedness Pulse Survey. (PricewaterhouseCoopers, January 2017). www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/pwc-gdpr-series-pulse-survey.pdf.
42 Ramnath K. Chellappa. "Intermediaries In Cloud-Computing: A New Computing Paradigm." (INFORMS Annual Meeting, Dallas: 1997).
43 Dave Bartoletti, Lauren E. Nelson, Liz Herbert, Paul Miller, Charlie Dai, Andras Cser, Andre Kindness (With: Glenn O'Donnell, William McKeon-White, Peggy Dostie.) "Predictions 2018: Cloud Computing Accelerates Enterprise Transformation Everywhere." (Forrester, November 2017). go.forrester.com/blogs/predictions-2018-cloud-computing-accelerates-enterprise-transformation-everywhere.
44 "Adoption Of Cloud Services In North America." North American Cloud Adoption Survey. (Evolve IP, 2017).
45 "Cloud: Driving Business Transformation." White Paper Number 20 (Cloud Industry Forum, March 2017).
46 "Toward New Possibilities In Threat Management: How Businesses Are Embracing A Modern Approach To Threat Management And Information Sharing." Global State Of Information Security Survey. (PricewaterhouseCoopers, 2017). www.pwc.com/gx/en/issues/cyber-security/information-security-survey/assets/gsiss-report-cybersecurity-privacy-possibilities.pdf.
47 McAfee Labs "2017 Threats Predictions" (Intel Security, November 2016). www.mcafee.com/us/resources/reports/rp-threats-predictions-2017.pdf.
48 "Ransomware: How Consumers And Businesses Value Their Data." (IBM X-Force Research, December 2016).
49 www.ibm.com/blogs/nordic-msp/ibms-ceo-on-hackers-cyber-crime-is-the-greatest-threat-to-every-company-in-the-world
50 hackernoon.com/ai-by-default-the-future-of-consumer-products-787273933362
51 John Gantz, David Reinsel, John Rydning. "Data Age 2025: The Evolution Of Data To Life-Critical" International Data Corporation (IDC) (April 2017).
52 TechValidate, "Privacy In The Digital Era: Are You Ready?" (ForgeRock, March 2016). www.forgerock.com/app/uploads/2015/10/Privacy-in-the-Digital-Era-Survey-Report.pdf.
53 Simon James Walker, Bart Willemsen. "The Impacts Of The General Data Protection Regulation On MDM." Gartner (June 2017). www.gartner.com/doc/3738054/impacts-general-data-protection-regulation
54 RiskIQ Threat Research, (October 2017). www.riskiq.com/blog/external-threat-management/gdpr-analytics-solution.
55 www.prnewswire.com/news-releases/the-media-trust-launches-an-industry-first-digital-vendor-network-to-enhance-gdpr-compliance-for-enterprise-digital-ecosystems-300518406.html.
56 Keynote Presentation At The 2013 FFWD Advertising & Marketing Sponsored By The Institute of Communication Agencies (February 2013). www.ogilvy.gr/bold-ogilvy/next-revolution-will-be-psychological-not-technological

57 James Manyika, Sree Ramaswamy, Somesh Khanna, Hugo Sarrazin, Gary Pinkus, Guru Sethupathy, Andrew Yaffe. “Digital America: A Tale Of The Haves And Have-Mores.” McKinsey Global Institute (McKinsey&Company, December 2015).
58 James McCormick, Brian Hopkins, Ted Schadler. “The Insights-Driven Business” (Forrester, August 2016).
59 www.merriam-webster.com/dictionary/culture.
60 Eurostat, July 2017. ec.europa.eu/eurostat/statistics-explained/index.php/Population_and_population_change_statistics#Further_Eurostat_information
61 United States Department Of Commerce: US Census Bureau, October 2017. www.census.gov/topics/population.html
62 “Schengen Area” Migration And Home Affairs (European Commission). ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/schengen_en
63 Directorate-General For Communication. How The European Union Works: Your Guide To The EU Institutions. Edited By European Commission. (Luxembourg: Publications Office, March 2015).
64 “Eurozone Fast Facts” CNN Library (January 2017). www.cnn.com/2013/07/09/world/europe/eurozone-fast-facts/index.html
65 europa.eu/european-union/about-eu/money/euro_en

Promotional Products Association International (PPAI) is the trusted leader delivering essential knowledge, resources and community to ensure the success of its members and the promotional products industry itself. With more than 14,500 member companies worldwide (based on 2017 figures), PPAI has served supplier, distributor and business service companies since 1903.