ARTICLE

The new European Union General Regulation on Data Protection and the legal consequences for institutions

Efrén Díaz Díaz

Bufete Mas y Calvet (law firm), Madrid, Spain

ABSTRACT

The aim of this study is to set out the new legal framework that has appeared in the European Union following the repealing of the 1995 European Directive on Data Protection on approving the new and significant General Data Protection Regulation (GDPR). This study provides an overview and a more detailed examination of the topic, based on an analysis of the legal framework established by the Directive in 1995 and the regulation proposals of 2012 that emerged in Europe and in the United States, followed by a study of the principal reforms contained in the GDPR of 2016. The study is concluded by identifying the most significant practical applications. The GDPR implies very important new rules that will be applied across the EU and that will directly affect every Member State. Furthermore, its aim is to overcome the existing fragmented regulations and to modernise the principles of privacy in the European Union. The practical and social implications of the GDPR are very significant, as it constitutes a single and updated set of rules applicable in the whole of the EU and for all the data processing of European citizens. It seeks to avoid the fragmentation of the EU market and to facilitate cross-border business and corporate activity, the free circulation of personal data and a greater guarantee of the fundamental rights and freedoms of European citizens. In the interest of European citizens, it regulates the rights to access, rectify, delete and object and it recognises two new rights: to be digitally forgotten and data portability.

1. Introduction: focus, methodology and scope

The focus of this study is to set out the new legal framework that has arisen in the European Union following the repealing of the 1995 European Directive on Data Protection on the approval of the new and significant General Data Protection Regulation (GDPR) (European Parliament and Council, 2016).

This study aims to provide an overview and a more detailed examination of the topic, based on an analysis of the legal framework established by the 1995 Directive followed by the regulation proposals of 2012 that emerged in Europe and in the
United States. This is followed by a study of the principal reforms set out in the GDPR of 2016 that were groundbreaking in the digital market and in the regulation of new rights, and concludes with setting out the most significant practical applications: from the subjects under obligation to the most significant issues for citizens, companies and the public sector.

The GDPR comprises very important innovative rules that will be applied across the European Union and will directly affect every Member State. Furthermore, its aim is to overcome the existing fragmented regulations and to modernise the principles of privacy in the European Union.

The practical and social implications of the GDPR are very significant, as it constitutes a single and updated set of rules applicable in the whole of the EU and for all the data processing of European citizens. It seeks to avoid the fragmentation of the EU market and to facilitate cross-border business and corporate activity, the free circulation of personal data and a greater guarantee of the fundamental rights and freedoms of European citizens. In the interest of European citizens, it regulates the rights to access, rectify, delete and object and recognises two new rights: to be digitally forgotten and data portability.

2. Background

2.1. The 1995 Data Protection Directive

The Directive 95/46/CE (Directive 95/46/CE of the European Parliament and of the Council of 24 October 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995) (European Parliament and Council, 1995), after 20 years in force, has now been replaced by a new, coherent and harmonious legal framework, to safeguard the fundamental right to data protection in the European Union.

The inconsistencies in data protection across the Member States of the EU have also been highlighted to the European Commission, the necessity for a single and harmonious regulation of data protection covering the whole of the territory of the EU, in particular in order to remove or reduce the margin of choice for national legislators, controlling authorities and the Courts.

In awareness of the problem posed by the fragmentation of data protection regulations in Europe and the different legislation and application of the regulation between Member States, the Court of Justice has reiterated the importance of the objectives pursued in Directive 95/46/CE, centring on maintaining a balance between the free movement of personal data and the safeguarding of the right to privacy (4/European Court of Justice, 2003).

However, Directive 95/46/CE did not fully guarantee any of its main aims.

Firstly, the right to personal data protection, established in article 8 of the European Charter of Fundamental Rights (European Parliament and Council, 2010), has not guaranteed the same level of protection either across all Member States or in the different entities and corporations. The rapid development of information and communication technologies has been a significant contributing factor by facilitating
the instant communication of personal data beyond national and European Union borders.

The effective application of the protective regulations on privacy, specified in a citizen’s right to control their personal data, has made it necessary for a greater level of cooperation between the supervisory data protection authorities of the different Member States. Likewise, the European Union is now better able to safeguard the rights of European citizens and in addition, to address the matter of data protection outside the borders of the European Economic Area (EEA)\(^2\), rather than the individual initiatives adopted by each Member State.

Secondly, the diversity of national approaches on the effectiveness of personal data protection has been an obstacle to the development and expansion of the internal market. As highlighted by the Court of Justice in the Lindqvist Sentence of 2003, the differences between the national regimes for handling data protection can seriously affect the establishment and functioning of an internal market.

Faced with this situation, in the European Union it has been necessary to establish a more transparent regulation and a more harmonious application of European Law, which imposes the same obligations on data controllers and processors, coherent supervision and the same sanctions across the EU. Together with the current disparities that prevent multinational organizations from developing pan-European policies on data protection, the diversity of operators, particularly social and economic, have made it necessary for greater legal security enabling data transfer across internal borders of the EU, something that was incompatible with the current fragmented national legislations.

Today the development of the digital economy in the European Union requires a coherent and legally harmonious framework for data protection in all Member States. Furthermore, the economic and social integration that has resulted from the functioning of the internal market has led to a substantial increase of cross-border flows and has resulted in an exchange of data between economic, social, public and private operators.

The need to guarantee the fundamental right to personal data protection and a uniform application in all EU policies has led the Commission to propose ‘a comprehensive and coherent approach guaranteeing that the fundamental right to data protection for individuals is fully respected’ (European Commission, 2010).

Accordingly, even though the current legal framework continues to be adequate with regards to aims and principles, it has not avoided a fragmented application of the fundamental right to personal data protection in the EU, nor legal uncertainty, nor the general public opinion that significant risks exist especially with regard to online activity (European Commission, 2010).

As highlighted in the Proposal for General Data Protection Regulation (European Commission, 2012), ‘those developments require a strong and more coherent data protection framework in the Union, backed by strong enforcement, given the importance of creating the trust that will allow the digital economy to develop across the internal market. Natural persons should have control of their own personal data. Legal and practical certainty for natural persons, economic operators and public authorities should be enhanced’.
2.2. Proposal for a General Data Protection Regulation (2012)

The European data protection reform is a legislative package that was proposed by the European Commission in 2012 to update and modernise the data protection regulation. It affects two legislative instruments: the General Data Protection Regulation is set to substitute Directive 95/46/CE; and the Data Protection Directive in the judicial and police area is set to substitute the Framework Decision on data protection of 2008, the object of the ‘Third Pillar’.

This study centres on the General Regulation as it has greater impact on the protection of privacy of natural persons and the practical legal repercussions for citizens and entities.

However, it is important to clarify that the Data Protection Directive in the police sector is aimed at protecting the personal data processed not only for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal sanctions, but also with a view to protection and prevention in the face of threats to public security. The guarantee of a consistent and high level of personal data protection for natural persons is fundamental, whilst at the same time, facilitating the exchange of personal data between the police authorities of the different Member States. The new Directive will be applied to cross-border personal data processing in the same way as within national boundaries by the police and judicial authorities. The current Framework Decision that will be substituted by the new Directive, only covered the cross-border exchange of data.

Following years of legislative work, in April 2016, the European Parliament approved the Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR), which came into force 20 days following its publication in the Official Journal of the European Union on 25 May 2016 (European Commission, 2016). Its provisions will be applied directly in all Member States in two years’ time on 25 May 2018. The countries will have a period of two years to pass the regulatory changes into national legislation.

The General Regulation is intended to establish harmonious regulation across all the Member States, and as a consequence, the repealing of the specific national regulations. It is based on the application of the principle of subsidiarity of Member State legislation, with the aim of overcoming the fragmented approach of Directive 95/46/CE.

The GDPR incorporates a single set of rules applicable in the whole of the EU and aims to update the regulatory framework, due to the profound changes, which have taken place with regard to how personal data is collected, stored and processed.

The Regulation maintains the rights to access, rectify, delete and object, and incorporates two newly created rights: the ‘right to be forgotten’ (or erasure) and the ‘right to data portability’. Furthermore, it addresses new issues such as the creation of profiles or pseudonymisation, and incorporates the principles of risk analysis and ‘privacy by design and by default’. The scope of application of the GDPR will extend beyond the borders of the EU and will affect organisations, entities and companies which even though they are not established in European territory, offer goods and services
to residents in the EU or monitor their patterns of behaviour (European Commission, 2010).

As stated in an official Communication, ‘the European Commission is now proposing a strong and consistent legislative framework across Union policies, enhancing individuals’ rights, the Single Market dimension of data protection and cutting red tape for businesses’ (European Commission, 2012).

This Communication also advocates data protection in a globalised world and states that ‘Individuals’ rights must continue to be ensured when personal data is transferred from the EU to third countries, and whenever individuals in Member States are targeted and their data is used or analysed by third country service providers. This means that EU data protection standards have to apply regardless of the geographical location of a company or its processing facility’ (European Commission, 2012).

The European Commission is also fully aware that in today’s globalised world, personal data are transferred across an increasing number of virtual and geographical borders and is stored on servers in numerous countries. Consequently, it is necessary to update the scope and reach of the European regulations to be applied in this matter.

In the end, as asserted in one of the first conclusions of the European Commission, ‘The EU data protection reform aims to build a modern, strong, consistent and comprehensive data protection framework for the European Union. Individuals’ fundamental right to data protection will be reinforced. Other rights, such as freedom of expression and information, the right of the child, the right to conduct a business, the right to a fair trial and professional secrecy (such as for the legal profession), as well as the status of churches under Member States’ laws will be respected.’ (European Commission, 2012).

The technological and legal challenges now faced in view of the development, expansion and popularisation of the Network of networks and its numerous technological applications necessarily requires a global approach because of its cross-cutting nature and international scope. Over the coming years we will, without doubt, be witnessing the most in-depth privacy regulation seen so far with new legal rulings as well as the recognition of fundamental rights and principles of data quality and their legitimate authorised processing. The motivation behind this new European ruling comes from the urgent need for a stable regulation which corresponds to future societies in digitalized environments with massive cross-border data processing.

The current revision of international privacy principles extends to all levels of government and organisation, not only in Europe, but also in international, sectoral and corporate areas.

In this sense, the global privacy framework is still defined by the principles of each society being democratic and respectful of the fundamental rights, since without privacy ‘we can talk about neither respect for dignity nor freedom’ (Piñar Mañas, 2008a). Furthermore, today privacy is subjected to numerous tensions, even challenges, with regards to the freedom of expression, the transparency of and access to information, the interests and evolution of the markets and the battle for public security (Piñar Mañas and Canales Gil 2008).
2.3. Privacy regulation in the United States

The original concept of ‘privacy’ was developed by the judges Warren and Brandeis in their well-known article, ‘The Right to Privacy, in which they stated, ‘In every such case the individual is entitled to decide whether that which is his shall be given to the public. No other has the right to publish his productions in any form, without his consent’ (Warren and Brandeis 1890).

Following an explanation of how exercising the law must be tempered by due deliberation of any other concurrent laws, both Magistrates concluded, ‘The principle which protects personal writings and any other productions of the intellect or of the emotions, is the right to privacy, and the law has no new principle to formulate when it extends this protection to the personal appearance, sayings, acts, and to personal relation, domestic or otherwise’.

This concept, which it is still well worth taking into account, has since been developed following the modern regulations on privacy and personal data protection. However, at that time, Warren and Brandeis found themselves in a difficult personal situation and the wife of one of them had her personal life invaded by numerous journalists. As a result, the Magistrates formulated a very interesting eloquent new law:

‘This development of the law was inevitable. The intense intellectual and emotional life, and the heightening of sensations which came with the advance of civilization, made it clear to men that only a part of the pain, pleasure, and profit of life lay in physical things. Thoughts, emotions, and sensations demanded legal recognition, and the beautiful capacity for growth which characterizes the common law enabled the judges to afford the requisite protection, without the interposition of the legislature’.

Initially privacy law only came in to play with regard to physical interferences in life and property. Gradually and since the mid-twentieth century, the object of the laws has been amplified and now, the right to life has gone on to mean the right to enjoy life, which includes the right to be alone.

As maintained by Piñar Mañas, ‘the law should preserve us in face of the invasions of the ‘sacred limits of our private and domestic life’. The right to privacy therefore supposes the right to be able to be alone, as far as each person desires, including completely alone, without suffering unwanted encroachment and without interfering in the rights of others’ (Piñar Mañas, 2008b).

These background facts are worth taking into account as they provide a context to the current regulation in the U.S.A on the issue of general privacy and personal data protection, in particular, for the influence that they also exercise outside the U.S.A.

2.3.1. Consumer Privacy Bill of Rights

2.3.1.1. Comprehensive bill for consumer rights On 23 February 2012, the Government of the United States of America approved the Consumer Privacy Bill of Rights (United States and White House Office, 2012), the result of a direct legislative reaction, of less than a month, following the approval of the European proposal on 25 January 2012 of the General Data Protection Regulation.

Whereas the Consumer Privacy Bill of Rights establishes clear rules for consumers in the Digital Economy and is inspired by the principles of security, confidence and
innovation, the Proposal for the General Regulation reaffirms the safeguarding of an adequate level of citizens’ privacy in the whole of the European Union, together with the recognition of rights to access, rectification, deletion and objection, and the regulation of new rights such as the digital right to be forgotten (article 17 of the GDPR) and data portability (article 18 of the GDPR).

However, even though the European Commission and the U.S.A have agreed upon a new framework for transatlantic data flows, known as ‘Privacy shield EU – USA’, the relationships between the European Union and the United States of America, on the matter of privacy, are at a delicate point.

The Consumer Privacy Bill of Rights forms part of a comprehensive US project to improve protection of consumer privacy rights and to ensure that the Internet continues to be the motor for innovation and economic growth. The legislative project will give users in the U.S.A more control over how their personal information is used on the Internet and to help companies to maintain consumer confidence and to grow in a rapidly evolving digital environment.

Furthermore, the main Internet companies and the online advertising companies have signed up to the ‘Do Not Track’ technology on the majority of the main Internet search engines in order to facilitate consumers’ control over online tracking. The companies responsible for publishing more than 90% of the advertising based on the behaviour of users online, such as Google, Yahoo!, Microsoft and AOL, have agreed to comply with it when consumers opt to control their online tracking.

The companies that sign up to this commitment will be subject to supervision by the Federal Trade Commission (FTC).

‘American consumers can’t wait any longer for clear rules of the road that ensure their personal information is safe online’, President Obama stated. ‘As the Internet evolves, consumer trust is essential for the continued growth of the digital economy. That’s why an online privacy Bill of Rights is so important. For businesses to succeed online, consumers must feel secure. By following this blueprint, companies, consumer advocates and policymakers can help protect consumers and ensure the Internet remains a platform for innovation and economic growth’ (The White House, 2012).

Within this framework, the US advertising industry also committed itself to not publishing consumers’ search data that the companies could use for purposes other than advertising, similarly for employers that make decisions on recruitment and insurers that determine cover.

As maintained by the president of the FTC, Jon Leibowitz, ‘It’s great to see that companies are stepping up to our challenge to protect privacy so consumers have greater choice and control over how they are tracked online. More needs to be done, but the work they have done so far is very encouraging’.

2.3.1.2. Consumer privacy draft bill The Consumer Privacy Bill of Rights seeks to establish a framework for safeguarding privacy and for promoting innovation in the global digital economy, and is aware that it plays a fundamental role in a sustainable economy and in the development of the knowledge society.

The starting point for this US regulation is the fact that millions of people every day go online to shop, do banking, learn, talk and work. The Internet has become a motor for innovation, business growth and job creation and so this regulation seeks
to establish a solid base of clear protections for consumers and a set of basic privacy principles and policies to guide businesses in their decisions in this evermore-strategic matter. In other words, the US draft bill fixes a base line of indispensable protections for consumers and increased security for companies.

2.3.1.3. Recognition of rights The new US ruling applies to personal data, understood to be any data, including bundles of data linked to an individual natural person. Personal data can be computer data or data on whatever other device.

The US Administration adopts the federal legislation that applies the principles of the Consumer Privacy Bill of Rights. Even without legislation, the Administration will set up a process so that multiple interested parties can use the rights set out in the new ruling as a model for codes of conduct that are required by the FTC.

These elements, ranging from the new Law and codes of conduct to related mechanisms will increase the interoperability within the framework for data privacy of US and international consumers. In particular, the Consumer Privacy Bill of Rights recognises the rights of consumers. These rights include the following:

1. individual control – consumers have a right to exercise control over the personal data collected by organisations and to find out how it is used;
2. transparency – consumers have a right to easily understandable information on privacy and security practices;
3. respect for context – consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data, and not for other or incompatible purposes;
4. security – consumers have a right to secure and responsible data processing on the platforms provided by the companies. These companies should assess the privacy and security risks associated with the use of personal data and maintain reasonable safeguards for controlling risk of loss, unauthorised access, destruction or modification and undue disclosure;
5. access and accuracy – consumers have a right to access the correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and at risk of adverse consequences to consumers if the data is inaccurate;
6. accountability – consumers have a right to have personal data processed only by companies that have the appropriate measures in place to ensure that they adhere to the law in force.

On 9 February 2016, the White House, by means of an Executive Order from President Barack Obama, constituted the Federal Privacy Council in the following terms: ‘There is hereby established the Federal Privacy Council (Privacy Council) as the principal interagency forum to improve the Government privacy practices of agencies and entities acting on their behalf. The establishment of the Privacy Council will help Senior Agency Officials for Privacy at agencies better coordinate and collaborate, educate the Federal workforce, and exchange best practices. The activities of the Privacy Council will reinforce the essential work that agency privacy officials undertake every day to protect privacy’ (The White House, 2016).
The Privacy Council, similar to the Supervisory Authorities established by the European Regulation, have as its main purpose to make recommendations to the Office of Management and Budget on Federal Government privacy policies and requirements, coordinate and share ideas, best practices and approaches for privacy protection and the application of adequate privacy safeguards; evaluate and recommend the best ways to address recruitment, training and professional development within the Federal Government with regards to the matter of privacy; and to carry out other functions related to privacy, according to the law, as indicated by the President.

2.4. The relevance of privacy in a global context

Privacy and data protection have therefore become a fundamental right in the European Union and a right for consumers in the US and their respective international areas of influence.

The origin and evolution of data protection certainly lies in the conflict that arises between computing and privacy, as recognised in the first national data protection laws and UN Resolution 45/95 (United Nations, 1995).

However, today the importance of data protection extends from the economic value of personal data to the significant construction of an internal market among the different Member States and in the global economy, as already highlighted by the promulgation of Directive 95/46/CE (European Parliament & Council, 1995) of the Parliament and Council on 24 October, relating to natural persons with regard to personal data processing and the free movement of data.

The global relevance was, without doubt, contributed to by the Joint Proposal for a Draft of International Standards On the Protection of Privacy with regard to the processing of Personal Data, set out in the Madrid Declaration on 5 November 2009 (International Conference of Data Protection and Privacy Commissioners, 2009).

The 35th International Conference of Data Protection and Privacy adopted the Resolution on anchoring data protection and the protection of privacy in international law, and resolves to call upon governments to advocate the adoption of an additional protocol to Article 17 of the International Covenant on Civil and Political Rights (ICCPR), which should be based on the standards that have been developed and endorsed by the International Conference and the provisions in General Comment No. 16 to the Covenant in order to create globally applicable standards for data protection and the protection of privacy in accordance with the rule of law (International Conference (35th) of Data Protection and Privacy, 2013).

The significance of data protection as a fundamental right in Europe and increasingly internationally has arisen from the European Union Charter of Fundamental Rights (European Parliament and Council (2010) and numerous judicial decisions from national and international courts, that have contributed to this right being enshrined as a power of disposition on one’s own personal data, (for example, in the Sentence of the Constitutional Court 290/2000))10.

Similarly, in the European Union, the so-called ‘European Model for Data Protection’ has been built on the following elements: firstly, data protection is a ‘fundamental and individual right’ and, unlike the right to privacy, forms an
essential part of European Union Law; data protection comes under the area defined by the Pillars of the EU, and lastly; data protection is built upon the important principle of exercising independent control as carried out by the supervisory authorities.

If these elements were not sufficient to understand the enormous and growing importance of privacy in the new world of digital globalisation, a brief analysis of some of the tensions that data protection law undergoes will clarify the depth of its repercussions and the importance of the issues also affected by privacy.

Firstly, the tension or challenge of ‘data protection versus transparency’ raises substantial issues that affect the relationships between people and public administrations and governments. Secondly, the challenge of ‘data protection versus national security’, even more relevant in the current climate of terrorist threats, affects very important matters of state and the constitutional obligations of protection and security of citizens and nations. Thirdly, the challenge of ‘data protection versus freedom of expression’ has new implications, not only because of the massive and widespread use of online social media, but also because of the legal, economic and reputational consequences, to name just the most evident, for national and international interests, which are difficult to control in a multinational and largely global scenario. Lastly, the challenge ‘data protection versus market’ not only hinders the economic, social and technological development because of fragmented regulations, but often it determines the recognized rights of citizens not only at a constitutional level but also in a hierarchy within the EU and internationally.

Finally, the relevance of privacy is evident when addressing the challenges of a right to online data protection when dealing with Cloud Computing, Social Networks, Online Behavioural Advertising (OBA) and Intellectual Property, Big Data, and leads to the adoption of new essential principles such as Accountability and Data Breach Notification amongst others, in a globalised framework which affects the determination of the applicable Law.

3. Main reforms of the General Data Protection Regulation (2015)

On 18 December 2015, the Committee of Permanent Representatives in the European Union (COREPER) confirmed the compromise texts agreed with the European Parliament on data protection reform. The European Council, Parliament and Commission reached a final agreement on 15 December 2015. Then the European Parliament approved the agreed text on 14 April 2016. This parliamentary approval brought to a close more than four years of work to drastically reform EU data protection regulations. Without doubt, the aim of the new General Regulation is to give people more control over their own private data in a world of smartphones, social networks, online banking and global transfers.

As the European authorities have underscored, ‘It is a fundamental agreement with important consequences. This reform not only strengthens the rights of citizens, but also adapts the rules of the digital age for companies, whilst reducing the administrative burden. These are ambitious and forward-looking texts. We can have full confidence in the result’ (Council of the European Union, 2015).
The protection of people with regard to their personal data processing is a fundamental right enshrined in The Charter of Fundamental Rights of the European Union (article 8), and in the Treaty on the Functioning of the European Union (article 16).

The aim of the GDPR is to improve the level of data protection for natural persons whose personal data is processed by automated means, or not, and to increase opportunities for trade and free movement in a single digital market, in particular, by reducing red tape.

For this reason it is useful to underscore the data that the European Council took into consideration when addressing this important reform: As many as 57% of Europeans consider that disclosure of personal data is an important issue; some 70% are concerned that companies can use their information for purposes other than it was collected for; only 15% consider that they are in full control of the information that they supply online; and 90% of Europeans believe that it is important for all the countries in the EU to have the same rights and protection (European Commission, 2015).

3.1. Level of data protection

The principles and regulations on personal data protection for natural persons are based on respect for fundamental rights and freedoms, in particular a right to protect data of a personal nature. This right has been reinforced in order to protect a natural person whose data is processed and to ensure that in practice they have greater control over their personal data.

As a result, the General Regulation follows these guidelines:

- It includes more specific rulings which allow data controllers and processors to process personal data, in particular, by gaining consent from the natural persons affected or any other legally entitled body, as well as a legal provision or contractual relationship.
- An improvement in the information supplied to data subjects about the specific purpose and destination of personal data when shared, in particular, the information for natural persons should be provided in simple and easily understood privacy policies or by means of standardized icons11.
- Personal data processing with regard to children under the age of 16, or in the case where the Law of a Member State indicates a lower age, but in no cases below the age of 13, will only be permissible if consent has been given or authorised by the child’s legal guardian.
- There is regulation of the information that should be provided when the data has not been directly obtained from the data subject.
- More easily accessible personal data for data subjects.
- The right of an individual to object to the processing of personal data on grounds relating to the particular situation of the data subject relating to public interest or the legitimate interest of the data controller. This right includes the use of personal data for the purpose of ‘creating profiles’.
- The right ‘to be forgotten’ (erasure, also in the sense of ‘de-listing’) concerning personal data, and that allows for example, that the persons in question can
demand the immediate erasure of personal data collected or published on social media or on a search engine\textsuperscript{12}.

- The right to portability must facilitate the transmission of personal data from one service provider such as a social network to another in a structured, commonly used machine-readable format. This will increase data protection rights and improve genuine competition between service providers.
- An obligation to give notice of the rectification, erasure or limitation of the data to each of the recipients of the data, unless this proves to be impossible or requires a disproportionate amount of effort.
- Common safeguards that affect data processing for archiving purposes in the public interest, scientific or historical research or for statistical purposes.
- The right to lodge a complaint before a supervisory authority and the right to an effective legal remedy against a supervisory authority in the national courts, regardless of the Member State in which the data processor is established.

### 3.2. ‘Digital single market’

The General Regulation establishes a single ruling, valid in the whole of the EU and applicable to personal data processing in the context of activities of an establishment of a data controller or data processor in the EU, regardless of whether the data processing is carried out in the EU or not.

In a technologically globalised world, extraterritorial application of the rulings presents a real challenge, as there would be little sense in their being limited to a specific space by the principle of territorial application of the Law, or to a certain set of people by application of the personality principle.

The General Regulation incorporates new rules about extraterritoriality and will be applied outside the European Union when personal data of EU residents is processed by data controllers or data processors who are not established in the EU and when the data processing is related to two areas: (a) the supply of goods and services to said data subjects in the EU, regardless of whether a payment is made by the data subject; or (b) behavioural monitoring, in as much as this takes place in the EU.

Therefore, the GDPR will be applied extraterritorially to personal data processing carried out by data controllers that are not established in the EU, but the national legislation of one Member State applies in accordance with the principles of public international law, for example, EU citizenship or residency or by applying diplomatic rules. In this way it avoids a situation where some contradictory national rules regarding data protection could disrupt cross-border data exchange.

It also envisages greater cooperation between Member States to enable a harmonious application of data protection rules in the whole of the EU. This will create fair competition and will encourage companies and entities, especially the small and medium-sized ones, to take maximum advantage of the digital single market (European Parliament, 2016)\textsuperscript{13}.

In order to reduce costs and create greater legal certainty, in important cross-border cases which involve various national control authorities, just one authority decision will be adopted. This ‘one-stop-shop system’ means that an establishment located in various Member States only has to deal with the data protection authority
relating to its main establishment and not with all the authorities in all the Member States where it is located\textsuperscript{14}. This system allows a single decision to be applied to the whole of the EU in case of disputes.

The Regulation is based on an approach that focuses on the risks with the aim of reducing administrative costs: the data controllers can put measures in place according to the level of risk involved in their data processing operations. Entities can carry out activities that infer varying kinds of risk to privacy, from the unlawful use of data without gaining explicit consent, to the excessive diffusion of personal data on the Internet, and also the transfer of personal data to entities or persons connected to the data controller. The GDPR does not offer a single solution that is valid for all the cases: the greater the risk to the personal data, the stricter the obligations.

As a result, the legal obligations of the data controller will be determined in accordance with the nature, area, context and the purposes of the data processing as well as the existing risks, of varying likelihood and seriousness, to the rights and freedoms of natural persons. Consequently, the data controller must put in place the appropriate technical and organisational measures to safeguard, and be able to demonstrate, that the data processing conforms to the Regulation. These measures will be reviewed and updated as necessary.

In addition, a ‘data protection impact assessment’ is set up when there is the likelihood that a kind of processing, in particular when using new technologies, is of a nature, scope, context or purposes that constitute a high risk to the rights and freedoms of people. For example, in the case of institutions that process sensitive data concerning health, religion, beliefs, minors, political allegiance or trade union membership, the system should be assessed to ensure compliance and the correct implementation of the technical and organisational measures necessary to safeguard the data protection for the owners of the information, especially in the case of data communication or transfer to other entities or third parties.

### 3.3. Improvement of instruments for safeguarding data protection

The Regulation sets out a series of measures to increase the data controllers’ responsibility and accountability in order to guarantee full compliance of the new data protection rules.

One of the most polemic issues has been the use of the adjective ‘explicit’ in the European Commission proposal, although in the end, the document returned to the use of ‘unambiguous’ which was already used in the Directive, with the aim of ensuring that in all cases consent is expressed by a clear affirmative declaration or act.

The data controllers, therefore, need to put a series of security measures into practice, including the obligation to notify of personal data violations in certain cases. In order that the rules contained in the Regulation stand the test of time and constant technological innovation, the principles of data protection ‘by design and by default’ are introduced so that the data controller complies with the requirements of the Regulation and to ensure that the rights of the data subjects are fully protected, (from the planning of the projects ‘by design’ and in any event ‘by default’.)
One of the notable measures set out in the GDPR is that the data controller and handler are obliged to designate a ‘data protection officer’ to ensure compliance with the Regulation in certain cases.

The data subjects, and in certain conditions the data protection organisations, can lodge a complaint with a supervisory authority or bring legal action if data protection rules are not complied with.

In the case of an infringement of the rules, the data controllers can face a fine of up to 20 million euros or 4% of their worldwide turnover for not complying with the decisions of the supervisory authority.

### 3.4. Safeguards for personal data transfer outside the EU

The GDPR contains rules governing the transfer of personal data to third countries and international organisations. These transfers can be carried out so long as a series of conditions and safeguards are complied with, in particular, when the European Commission has decided that there is ‘an adequate level of protection’.

New decisions on ‘adequate’ protection will need to be reviewed at least every four years. The existing authorisations and decisions taken will remain in force until their subsequent modification, substitution or derogation. Ultimately, the Regulation introduces a mechanism linked to periodic updating to prevent technological evolution from rendering legal safeguards useless and leaving citizens, in effect, unprotected.

The general principle of transfers determines that data transfers for processing in a third country or international organisation may only be carried out if the data controller and handler comply with the conditions of the rules, in particular with regard to further personal data transfers from the third country or international organisation to another third country or international organisation.

Therefore, as an example, to authorise a transfer from a document storage facility in the cloud, it will not be sufficient for the provider to claim that it is secure, but rather it is necessary to provide an accreditation that the appropriate safety measures have been implemented, and in the case of any successive international transfers to other providers that sufficient technological safeguards are in place.

The spirit and purpose of the Regulation seek to ensure that its rules offer maximum protection to individuals, so that in practice their non-compliance or impairment through conduct that disrupts the protective regime for international data transfers is prevented.

For this reason, the new transfers regulation system not only contemplates a sufficient level of protection but also includes clear rules to enable transfers with appropriate guarantees by binding corporate rules and includes significant exceptions to cover specific situations.

### 3.5. Principles

The GDPR formulates and updates the principles relating to personal data processing as follows. Personal data should be:

a. processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’);
b. 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 (‘purpose limitation’);
c. adequate, relevant and limited to what is necessary in relation to the purposes for
which they are processed (‘data minimization’);
d. 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 pur-
poses for which they are processed, are erased or rectified without delay
(‘accuracy’);
e. 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 proc-
essed 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 organisational measures
required by this Regulation in order to safeguard the rights and freedoms of the
data subject (‘storage limitation’);
f. processed in a manner that ensures appropriate security of the personal data,
including protection against unauthorised or unlawful processing and against
accidental loss, destruction or damage, using appropriate technical or organis-
ational measures (‘integrity and confidentiality’); and
g. The controller shall be responsible for, and be able to demonstrate compliance
with the rules (‘accountability’).

3.6. Data subjects’ rights

The General Regulation is inspired by real and effective personal data protection and
consists of a harmonious set of rights, not only recognising the existing rights in
international and national rules, such as access to and rectification or cancelation and
the right to object, but also by setting out two new laws: the digital ‘right to be for-
gotten’, also known as erasure (article 17 of the GDPR) and ‘data portability’ (article
18 of the GDPR).

3.6.1. Right to be forgotten

The setting up of the new Right to be Forgotten¹⁶ is covered in article 17 of the
General Regulation and is established for the first time as a right separate from the
so-called ‘ARCO rights’ (access, rectification, cancellation and opposition).

3.6.1.1. European jurisprudence prior to the General Regulation  At the beginning
of this study, there was a detailed examination of the legislative process leading
to the approval of the Proposal for a Regulation relating to protection for
natural persons with regard to personal data processing and the free movement of
such data.
The interesting point about this regulation is not only the enormous importance of its content, but also the point in time when it occurred. The fact that its elaboration in the European Parliament coincided with the preliminary hearing for the interpretation of ‘right to be forgotten’ in the Court of Justice of the European Union (CJEU) has led to a unique and historic situation. Since 2011 and 2012 the European legislative and judicial powers have both been debating and studying such an important right for European citizens at the same time. Judgements made in the CJEU have somehow set the pace of europarliamentary debate.

In 2012, Viviane Reding, the Vice-President of the European Commission and Commissioner for Justice, Fundamental Rights and Citizenship, proposed approval of the General Regulation for data protection and pushed for better protection of citizens’ data in circulation on the Internet and the ‘right to be forgotten’ with regard to the data that people post online.

With the aim of adapting to the demands of the Treaty of Lisbon, the European Commission’s proposal entails a new European legislative framework for personal data protection, the mainstay of which is that citizens can exercise effective control on the personal data that concerns them (Blume, 2012).

According to Reding, ‘in Europe we have various rights: a right to free press, or Internet if you wish: to information; a right to privacy and a right to intellectual property. None of these are absolute. Each one has to balance out with the others. The data protection rights of journalists are outside of this equation as they need to collect data to make news. This is different to the fact that I should wish that my personal data are protected and that I should have the right to recover them from where they are. I cannot change a story or History or intervene in a poem or a painting, or the files of a newspaper’ (el País Digital, 2012).

Previously, Vice-President Reding had pointed out that people’s rights need to be built on fundamental pillars, the first and most important of these being ‘the right to be forgotten’: a comprehensive set of existing and new rules to better cope with privacy risks online’. These new rules, in order to fully modernise the legislation, expressly include the right, and not only the ‘possibility’ for people to be able to withdraw their consent to data processing. For this reason, she maintained that, ‘the burden of proof should be on data controllers – those who process your personal data. They must prove that they need to keep the data rather than individuals having to prove that collecting their data is not necessary (...’).

The preliminary hearing for interpretation was based on and made direct reference to Directive 95/46/CE of the European Parliament and Council, of 24 October 1995, although it has been crucial in the parliamentary deliberations, where even in the final proposal, as mentioned earlier, the ‘right to be forgotten’, is rephrased more precisely as the ‘right to erasure’ (Official Journal of the European Communities, 1995).

Once the judgement was announced in the Grand Chamber of the Court of Justice (ECJ) on 13 May 2014, as it concerned a preliminary ruling sought by the Spanish National Court regarding the interpretation of legislation, the Spanish National Court proceeded to lift the suspension on the proceedings initiated by Google Spain, S.L., and Google, Inc.

Once the judgement from the European Court of Justice (ECJ) was received in Spain, the Member State that had first requested the ruling, the Spanish National
Court communicated this to the parties in the proceedings and requested that they make their allegations, and in some cases, to pronounce on maintaining evidence admitted by Google but not within the time limit.

Once the arguments had all been presented in the case regarding the judgement from the ECJ, the proceedings remained to be heard in November 2014, deliberations were concluded on 18 December 2014, and the Spanish National Court gave their judgement on 29 December 2014.

Prior to and at the same time as the case judged by the ECJ, it has been discovered subsequently that Google Spain, S.L., and Google, Inc., requested the withdrawal of the actions brought as soon as the cases were remitted for judgement, in accordance with art. 74.1 of Spanish Law 29/1998, of 13 July, regulating the contentious-administrative jurisdiction. These requests for withdrawals were admitted, prior to the proceedings, and affected more than 130 cases (Europa Press, 2015).

3.6.1.2. Concepts of ‘blocking’ and ‘erasure’ The GDPR defines the digital ‘right to be forgotten’ as ‘the right to obtain from the data controller the erasure of personal data concerning the data subject without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies’ which is strictly regulated in article 17 of the GDPR.

It is, therefore, essential to clarify the difference between the concepts. The concepts of ‘blocking’ and ‘erasure’ in the context of Spain, have been quoted for being amongst the most innovative, and some authors have gone on to say that ‘the (Spanish) draft Regulation included two definitions referring to blocking and erasure in the version submitted to public inquiry. Blocking was defined as ‘the identification and reserving of personal data in order to prevent its processing except in the case of allowing Public Administrations, Judges and Courts to attend to the possible responsibilities that have arisen from the processing and only for the corresponding limitation period. (...) Erasure was defined as ‘the physical elimination of the blocked personal data once the limitation period had expired’.

However, in the definitive legal text, such definitions were removed because of their lack of clarity and have been replaced by a new concept of ‘cancellation’. In article 5.1.b of the (Spanish) Organic Law on Personal Data Protection (RLOPD), cancellation is defined encompassing blocking and erasure in these terms: ‘a procedure by which the data controller ceases to use the data. Cancellation infers the blocking of data, consisting in their identification and holding in order to prevent it being processed except for being made available to Public Administrations, Judges and Courts to attend to the possible responsibilities that have arisen from the processing and only for the corresponding limitation period. Once this time period has expired the data will be erased.

In our opinion, this aspect is very pertinent to the analysis of the right to be forgotten, even though it has not been given the real importance that it deserves. As maintained by the Spanish National Court in repeated judicial decisions, ‘blocking will involve data being ‘locked up’, isolated or incommunicated in such a way that it is impossible for any further processing or use to be made of them, except in the cases indicated’. As a consequence, the differentiation between blocking and erasure has an enormous practical application in the area of de-listing in search engines.
Various authors have indicated that ‘cancelation is not the same as deletion; cancelation cannot demand total and absolute deletion of the data, even though blocking is necessary with all the security characteristics that must go with it’.

The Spanish Data Protection Agency (AEPD), a leader in the EU in this field, has specified that the exercise of these rights (of rectification or cancellation) implies stopping the processing and use of the applicant’s personal data by the controller of the file for which the request for cancelation has been made, and implies the blocking of the personal data by the entity owning the file and prevents the processing of these for promotional purposes.

Blocking should be regarded as the holding of the necessary data in order to attend to, whenever appropriate, the possible responsibilities deriving from the processing or the underlying relation to this, so that it should be possible for the judicial or administrative authority to access the data that had been processed and to be able to effectively assess the possible responsibilities demanded by the data subject or by the judicial or administrative authorities.

The data should remain blocked in the cases where cancellation has been requested by the data subject as well as by the data controller when faced with inaccurate or unlawful data processing, or once the final purposes which justified the processing have been completed.

The AEPD has analysed the characteristics of blocking in numerous reports (AEPD, 2007) and has indicated that ‘there will be cases in which the data should be cancelled whether because the data are no longer necessary for the original processing purposes, or whether the contract between the data controller and the clients has expired, the aforementioned cancellation should be carried out by means of blocking the personal data undergoing the processing and that produces similar effects as the physical deletion of the data, except in certain circumstances, as described in article 16.3 of the Organic Law, does not automatically infer that deletion.’

During the blocking, the data remain available for Judges, Courts and Public Administrations, although their ‘active’ processing is not possible. With regard to how the blocking is carried out, the AEPD specifies that ‘it should be carried out in such a way so that access to the data is limited to the purposes covered by the non-physical erasure of the data in question. In this way, even though the data can still be processed, access to them will remain completely restricted, in accordance with the purposes indicated in the previous rules’.

These issues are not simply theoretical disquisitions but are also of practical interest. In article 17, paragraph 2 of the GDPR, picking up on the previous concepts, it states that, ‘Where processing has been restricted under paragraph 1, such personal data shall, with the exception of storage, only be processed with the data subject’s consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State’.

3.6.1.3. Legal configuration of the new right The new configuration of the digital right to be forgotten transcends the content of the right to cancellation in the digital environment, as it has been applied in compliance with the European Privacy Directive and the national laws.
The digital right to be forgotten, for example, overcomes the necessity of request-
ing that the owner of the website carries out the prior or simultaneous deletion of
certain information that is unsuitable and excessive, in order to request its later de-
listing. As a consequence, as recognised by the EJC in the judgement of 13 May 2014,
the operator of a search engine is obliged to remove from the list of results displayed
following a search made on the basis of a person’s name, links to web pages published
by third parties and containing information relating to that person, also in a case
where that name or information is not erased beforehand or simultaneously from
those web pages, and even, as the case may be, when its publication in itself on those
pages is lawful\(^23\).

In practice, this law has a dual dimension: on the one hand, it recognises the cit-
izen’s demand for the information affected to be immediately deleted on the website,
and to prevent it from being diffused if the data subject makes the request. This right
can be exercised by the citizen in those cases where the processing does not comply
with the law, when there is an objection on personal grounds or if consent for the
processing is withdrawn, or when the data are not necessary for the purposes for
which they were collected, or the expiry of the personal data storage time limit.

If during the course of data processing the entity, corporation, website, social net-
work or ultimately the data processing controller should make the data public, this
controller will be obliged to adopt the necessary measures, not only organisational,
but also the appropriate technical ones in order to inform third parties of the data
subject’s request for cancellation in order that the data be erased.

It is worthy of note that this right impinges on the role of the data Controller, that
is the entity, corporation, website or social network that processes the data. The data
Controller should choose between restricting the processing (article 17 bis GDPR), or
erasing the information immediately (article 17 GDPR), each case being weighed up
on a case by case basis regarding the scope of this right as opposed to the right to
freedom of expression, public health, the duty to store data to comply with legal obli-
gations and the public interest\(^24\).

### 3.6.2. Right to data portability

Data portability is the other new right recognised in article 18 of the GDPR. The data
subject has the right to ‘receive the personal data concerning him or her, which he or
she has provided to a controller, in a structured, commonly used and machine-read-
able format and have the right to transmit those data to another controller without
hindrance from the controller to which the personal data have been provided’.

There is not as much jurisprudence surrounding the right to data portability as the
digital right to be forgotten and it has arisen mainly for reasons of technical inter-
operability.

However, the General Regulation already envisages that exercising this right does
not prejudice the digital right to be forgotten and erasure that are regulated in article
17. In practice it will be necessary to weigh up this right with the cases of data proc-
essing that are necessary to perform tasks in the public interest (e.g. in the case of
tax, geographical or judicial authorities) or the intrinsic rights vested in the data
controller to exercise powers of governing bodies (e.g. in exercising expropriations or sanctions).

In addition to these two new laws is a greater general awareness regarding online privacy, the effective application of ‘privacy by design’ in the development of products, applications and solutions, as well as the establishment of the obligation on the data Controller to carry out impact assessments on personal data processing, including codes of conduct.

The legal instruments that complement the exercising of ARCO rights and the two new rights set out in the GDPR provide citizens with more effective safeguards of their privacy as the data subjects will dispose of better guarantees to be able to defend and protect them.

3.6.3. Minors

The area relating to minors is one of the most delicate and acute within Data Protection and considerable attention has been paid to it since the new Draft Regulation, not only in establishing the principles such as, for example, data quality and qualification for processing, but also in the ruling contained in article 8 of the GDPR concerning the ‘conditions applicable to a minor’s consent in relation to information society services’.

These rules can similarly be applied to other areas directly related to children such as data processing concerning matters of testamentary dispositions, health or ideology, religion and beliefs of the minors.

And so, in relation to the direct offer of services to minors in the information society, data processing will only be lawful where the child is at least 16 years old, or in the case where the Law of a Member State sets out a lower age, but under no circumstances younger than 13 years old, if consent is given or authorised by the holder of the parental responsibility for the child.

Although technically there are still difficulties involved in age verification, the GDPR obliges the data controller to carry out reasonable efforts to verify that consent has been given or authorised by the holder of the parental responsibility for the child.

The direct application of these rules in the area of privacy will not affect general contract law in Member States such as the rules on the validity, formation or effect of a contract in relation to a child, where the principle of lex specialis derogat generalis is applied (Fellmeth & Horwitz, 2009).

In the same way, consideration number 38 makes a particular reference to minors, with the aim of assuring adequate protection of their privacy with regard to the risks that children are exposed to today: ‘Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child.’
Further innovations are to be found in the principle of transparency which is equivalent to the right to information that is currently in force. Consideration number 58 of the GDPR regulates this principle with regard to the principle of data quality, according to which the data controller is obliged to collect only the data necessary for the purposes that they are collected and paying attention to the state of technology at the time the data was collected. According to Consideration number 58, ‘The principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used. Such information could be provided in electronic form, for example, when addressed to the public, through a website. This is of particular relevance in situations where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him or her are being collected, such as in the case of online advertising. Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand’.

In the area of the right to be forgotten, the Regulation considers how this can be applied to minors, including when they are no longer minors regarding preterit information. In Consideration number 65, it is underscored that, ‘That right is relevant in particular where the data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet. The data subject should be able to exercise that right notwithstanding the fact that he or she is no longer a child. However, the further retention of the personal data should be lawful where it is necessary, for exercising the right of freedom of expression and information, for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, on the grounds of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defence of legal claims.’

3.7. Regulatory compliance

The General Regulation establishes the naming of a Data Protection Officer (DPO) to help the competent authorities in safeguarding that the data protection regulation is complied with.

Another instrument for safeguarding compliance is the Privacy Impact Assessment (PIA), which applies in cases where there is likely to be a high risk to the rights and freedoms of natural persons. In these cases the competent authorities shall carry out a prior or simultaneous impact assessment of a particular processing, especially when a new technology is used.

3.7.1. Data Protection Officer

The figure of the Data Protection Officer has been the subject of intense debate regarding its obligatory and universal nature for all entities and institutions. In the
end, the DPO will be a voluntary instrument for the data controller and processor, although with some exceptions, with a view to ensuring legal and technical compliance in entities.

It is important to point out that the Data Protection Officer is a necessary figure in entities, companies, institutions or any agent that carries out automated, or non-automated, processing of personal data. In practice, the DPO would be the person who deals with data protection and privacy matters, however, his or her designation does not exonerate the institution or organisation of the responsibility for what is done with the personal data or of complying with the rules of the Regulation.

Organisations and public institutions and entities with more than 250 workers are obliged to hire a Data Protection Officer. In the case of entities with less than 250 employees, a DPO will be obligatory when they need to carry out a systemic and periodic tracking of the personal data processed for monitoring or market research, risk analysis or credit data or solvency, and also when treating data classified as requiring high protection.

Entities can specify and expand the functions and responsibilities of the Data Protection Officers, but the tasks of the DPO should at least include the following:

a. to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;

b. to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;

c. to provide advice where requested as regards the data protection impact assessment and monitor its performance;

d. to cooperate with the supervisory authority;

e. to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation, and to consult, where appropriate, with regard to any other matter.

The data controller and processor are obliged to designate a data protection officer in order to ensure compliance with the regulation when the processing is carried out by a public authority or body, except for courts acting in their judicial capacity; the core activities of the controller or the processor consist in processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring on a large scale of data subjects; or when there is large scale processing of data in the special categories (ethnicity or race, political opinions, religious or philosophical convictions, trade union membership, genetic data relating to biometrics, health, life, sexual orientation and data relating to criminal convictions and offences).
The incorporation of a DPO is intended to strengthen the figure of the Safety Officer, the person currently assigned in organisations to ensure the compliance of the data protection regulation.

The most significant difference between the Security Officer and the Data Protection Officer is that the latter has exclusive functions. The DPO will no longer be the person who has been designated up until now as Safety Officer, with hardly any justification, resulting in a person being chosen without the appropriate skill set. The DPO will be designated according to their professional aptitudes and in particular, their specialist knowledge of the data protection legislation and practices, and their ability to carry out the obligations set out in the GDPR. The DPO can be part of the staff of the controller or the processor or carry out these functions as part of a services contract. The data controller or processor will publish the contact details of the DPO and will send them to the supervisory authority.

The GDPR clearly states that the data controller or processor shall ensure that the DPO does not receive any instructions regarding the exercise of those tasks. The DPO shall not be dismissed or penalised by the controller or the processor for performing his tasks. The data protection officer shall directly report to the highest management level of the controller or the processor.

3.7.2. Impact on privacy assessment

The surge of new business models, means of communication and technological media such as wearables, the rise of the Internet of Things (IoT), the increasing use of Big Data, the processing of sensitive data relating to religion, ideologies, biometrics; geolocalisation, new frontiers of cybersecurity, even fingerprinting and facial recognition technology on social networks, give rise to new risks that can have simultaneous consequences in different locations; all of these factors confirm the value of developing this unified Europe-wide framework.

In article 33, the General Regulation sets out the requirement for a data protection impact assessment when it is likely that a kind of processing, in particular when new technologies are used, or the nature, scope, context and purposes for processing pose a high risk to the rights and freedoms of people. In these cases, the data controller is obliged to carry out an assessment, prior to processing, of the impact of the planned personal data processing operations. A single assessment will serve for a series of similar processing operations that present similar elevated risks. The data controller will collect the assessment from the DPO once the data protection impact assessment has been completed.

A data protection impact assessment shall be required in the following cases:

a. a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

b. processing on a large scale of special categories of data, or of personal data relating to criminal convictions and offences

c. a large scale systematic observation of an area accessible to the public.
The assessment shall contain at least:

a. a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
b. an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
c. the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

3.8. Sanctions

Another significant aspect to take in to account is sanctions. The new Regulation seeks to harmonise the criteria for sanctions across the EU and also to increase them in order to safeguard greater protection of a fundamental right such as privacy.

And so the range of sanctions against data controllers and processors that fail to comply with the regulation has been increased and the national data protection authorities are empowered to apply administrative sanctions that can include fines of up to 20 million euros, or in the case of entities, up to 4% of annual worldwide turnover of the previous financial year, whichever amount is higher.

Furthermore, the affected party has the right to present a claim to the national supervisory authority as well as their right to effective legal protection from any of the Member States.

For many organisations these sanctions would have a very hard economic impact which can be avoided by taking the correct preventive legal and technical measures in good time.

3.9. Supervision and compensation

The General Regulation reinforces the position of the Supervisory Authorities as independent and specialised entities for protecting data protection rights. Their powers are expanded and harmonised, particularly by means of a recognised general sanctioning authority.

Furthermore, mechanisms for cooperation and coordination between the Supervisory Authorities are also established, the main exponent of which is the European Data Protection Council, successor to the current Working Group of article 29, with additional roles and capabilities.

Despite these significant advances, the activity of the Supervisory Authorities will largely depend on how the new ‘one-stop-shop mechanism’ works. In its original design, the mechanism consisted of a single authority with various establishments in the Union. This option that was applauded by some and criticised by many posed serious problems to the effective protection of citizens’ rights.

The final result, following complex negotiations, appears to be positive insofar as it uses solutions that allow for direct participation from the data protection authorities.
to defend the data subjects in its Member State. It may however turn out to be excessively complex and contain some elements that are difficult to apply in practice, especially due to the necessity of coordination between the authorities concerned.

4. Practical applications

4.1. Who the new Regulation affects, and how

The new Regulation affects all entities that collect and process personal data. Currently in the ‘information society’ it is practically universal that all entities and organisations use a database for contacts, members, clients, employees, and so on.

Entities that process sensitive data (regarding health, race, religion, sexuality, etc.), are particularly affected by the rules of the Regulation, for example, by the special requirements attached to the information and the consent of the data subjects that should be clearly expressed and therefore explicit, as well as other new elements such as the obligation to designate a Data Protection Officer.

One particular change is that the Regulation is now applicable to entities that, even without having set up an establishment in EU territory, direct their goods, services and activities at European users, independently of where the payment is made or where the main establishment is located.

The significance of this Regulation is all-encompassing as it substitutes Directive 95/46/CE and applies directly to all Member States. It is clear that it is of huge importance for all entities as this is the data protection regulation that is protecting citizens in general and, in particular, the affected data subjects.

4.2. Particular innovations for entities

The most significant innovations for entities that carry out systematic data processing are as follows:

1. The Regulation is directly applicable in all Member States of the EU, without the need to transpose rules into the domestic laws of each Member State. It constitutes a single data protection ruling for all the Member States of the EU.
2. The measures to be adopted and implemented are based upon the risks involved in personal data processing for the data subject. It will be necessary to designate a Data Protection Officer (DPO), carry out a Data Protection Impact Assessment (PIA) or even a consultation with the data protection authorities prior to the personal data processing if there is an elevated risk for the data subject, in the absence of the correct measures taken by the controller to mitigate them.
3. New principles of data protection: transparency, responsibility, data protection by design and by default.
4. Two new rights that the entities will safeguard: the right to be forgotten and data portability.
5. Special categories of sensitive personal data such as regarding health, race, sex, ideology, religion, beliefs, etc., and other new data such as genetic data and biometric data.
6. Consent for general personal data processing must not only be ‘express’ but rather ‘clearly unambiguous’ and, what is more, consent must be ‘explicit’ in the case of sensitive data that reveals ethnicity or race, political opinions, religious or philosophical convictions or trade union membership, or genetic data or biometric data which leads to the unequivocal identification of a natural person, data relating to the sex life or sexual orientation of a natural person. The controller will need to be able to demonstrate that the necessary consent was obtained from the owner of the personal data.

7. New possibilities have opened up for international transfer of personal data to third countries outside the EU or the European Economic Area (EEA) in view of a sector of activity such as Cloud Computing.

8. Measures for pseudonymisation and anonymisation of personal data: Pseudonymisation does not escape the provisions of the Regulation and they will remain applicable as it is possible to identify the person that the personal data refers to; anonymisation is not subject to the Regulation so long as it is irreversible and does not contain personal data.

9. Significant reduction in red tape for the entities: a system of one-stop-shop we be set up which serves the organisations as well as the data subjects as they will only have to liaise with one supervisory authority.

4.3. ‘Data Protection Officer’ (DPO)

The post of DPO is defined as follows for the entities:

1. They need to be professionally qualified and have specialist knowledge in the area of data protection.

2. Their role is basically to ensure that the data protection regulations are complied with by making this compatible with the functioning of the organisation, achieving the lawful and legitimate objectives of its activity and safeguarding the right to data protection and security; furthermore, the DPO will liaise with the Data Protection Supervisory Authority.

3. The implementation of a DPO is obligatory.

4. The DPO can be hired externally or be appointed from within the workforce of the organisation.

5. The following entities require a DPO:
   a. All public organisations, with the exception of the courts exercising their judicial powers,
   b. entities which carry out ‘profiling’ (registration and analysis of the psychological characteristics and behaviour of a person in order to assess or predict their abilities in a certain field or to help in identifying the categories of people),
   c. entities that require regular and systematic monitoring of the data subjects on a large scale (for solvency, market research or checks associated with productivity or risk analysis),
   d. entities that deal mainly with processing special categories of data (data that reveals race, ethnicity, ideologies, religion or philosophical beliefs, trade
union membership, genetic data and the processing of biometric data that can lead to the unequivocal identification of a person, as well as those relating to health, and life and sexual orientation, and data relating to convictions and criminal background) and when ordered by an EU or Member State Law.

4.4. Applicable solutions

The solutions should be tailored to suit every entity, case by case. It is not recommendable to adopt merely standard solutions as the initial low cost may turn out to be costly in the long run.

In relation to the volume of data processed or the sensitive nature of the data, every entity should hire suppliers that are accredited and professional.

A serious implementation of data protection must address the activity carried out by the entity, and within that, the processing of personal data of clients, employees, members, suppliers, etc., necessary for the purposes for which they were collected and also particular necessities such as in response to its strategies, activities and internal management.

It is recommended that each entity make a consultation according to their necessities. In principle, this need not imply an unsurmountable cost for the organisation, and it may also be an investment that results in gaining the loyalty of the data subjects and optimization of the organisation and productivity. The behaviour of citizens has evolved and they are worried that their data may not be safe, so it is necessary to look at it as a requisite for gaining the confidence of the data subject, and as an investment rather than a cost.

5. Conclusions

The recent approval of the General Data Protection Regulation holds positive prospects for the future of data protection in Europe. The existence of a solid and uniform legal framework across Europe that has been updated to meet the necessities of technology, will not only allow for the potential of the Digital Market to be freed up, for the promotion of innovation, for creation of employment and generation of wealth, but also for safeguarding the fundamental right of data processing protection for citizens or residents in Europe.

The Regulation sets out that entities and organisations comply with their obligations by adopting protectory measures according to the level of risk, carrying out impact assessments, better management of crises and incidences relating to cyber security, as well as by the implementation of legal and technical instruments that guarantee security, confidentiality and integrity of the personal data and of all associated information, and by recognising and addressing two new rights: the digital right to be forgotten and the portability of personal data.

Technical advances must go hand in hand with the definition of new alternative mechanisms which result in accessing and safeguarding the information, and also in transparency and in respecting the principles of data protection: purpose limitation,
data minimization, accuracy, storage limitation, integrity and confidentiality, and accountability.

The main innovations of the General Data Protection Regulation are:

1. New rights for citizens: the right to be forgotten and the right to a user’s data portability from one electronic system to another.
2. The creation of the post of Data Protection Officer (DPO).
3. Obligation to carry out Risk Analyses and Impact Assessments to determine compliance with the regulation.
4. Obligation of the Data Controller and Data Processor to document the processing operations.
5. New notifications to the Supervisory Authority: security breaches and prior authorisation for certain kinds of processing.
6. New obligations to inform the data subject by means of a system of icons that are harmonized across all the countries of the EU.
7. An increase in the size of sanctions.
8. Application of the concept ‘One-stop-shop’ so that data subjects can carry out procedures even though this affects authorities in other member states.
9. Establishment of obligations for new special categories of data.
10. New principles in the obligations over data: transparency and minimization of data.

The new regulation represents considerable advantages:

a. It will bring a harmonisation of the criteria for application and a safeguarding of the rights of European citizens in the area of privacy and data protection. This means that citizens will have greater control over their data. It is worth highlighting the pioneering nature of Europe in looking to safeguard these fundamental rights.
b. It incorporates the right to be forgotten and the right to portability.
c. It focuses on preventive measures rather than on sanctions affecting privacy from the design stage with ‘design by default’, impact assessments and codes of conduct and the necessity of a Data Protection Officer.
d. It contains new regulations for the supervisory mechanisms relating to the national authorities.
e. It includes a comprehensive sanctions system.
f. The European Council for Data Protection will be able to take legally binding decisions, also in the One-stop-shop, relating to the right to be forgotten.
g. Red tape will be reduced because it will no longer be obligatory for companies to register their filing systems with the national authorities.
h. For companies operating in the European Union, this new regulation will be an improvement upon the legislation in force up until now.

Notes

1. Today’s concept of privacy is rooted in the United States where, in 1888, the American Judge Cooley set the definition of privacy to be “the right to be let alone”
(Cooley, Thomas McIntyre, and John Lewis. 1907. "A Treatise on the Law of Torts or the Wrongs Which Arise Independently of Contract." Chicago: Callaghan & Co.) For this reason, a study of the European regulation requires knowledge of the origin of this important right which today, is recognised and consecrated as a fundamental and autonomous right in The Charter of Fundamental Rights of the European Union. 2010. CFRUE. http://www.boe.es/buscar/doc.php?id = DOUE-Z-2010-70003.

2. The European Economic Area (EEA) includes the States of the European Union, Island, Liechtenstein and Norway. http://www.europarl.europa.eu/atyourservice/es/displayFtu.html?ftuid=FTU_6.5.3.html.

3. The Third Pillar includes police and judicial co-operation in criminal matters, regulated by Title VI of the TUE ("DOUE" no. 83, of 30 March of 2010, Pages 47–199 (153 pages.), European Union Ref: DOUE-Z-2010-70006).

4. The legislative procedure and regulatory developments can be followed in the European Parliament, available at: http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2012/0011(COD)&l=en and in http://eur-lex.europa.eu/procedure/ES/2012_11?rid=1&qid=1443173807357.

5. European Commission (2010) "Special Eurobarometer 359. Attitudes on Data Protection and Electronic Identity in the European Union." http://ec.europa.eu/public_opinion/archives/eb_special_359_340_en.htm.

This study revealed significant information about the current scenario in Europe. Only 26% of users on social networks are in control of their data; 74% of Europeans consider that diffusion of personal information is a growing part of modern life; 43% of Internet users have requested more information than necessary; only 33% of Europeans know about the national data protection authorities. Notably, 90% of Europeans want the same data protection rights across the whole of the EU.

6. “Advocate General Considers EU-U.S. Safe Harbor to Be Invalid.” 2015. The National Law Review. http://www.natlawreview.com/article/advocate-general-considers-eu-us-safe-harbor-to-be-invalid http://curia.europa.eu/juris/document/document.jsf?text=&docid=168421&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=401385.

Decision of the Court (Grand Chamber) of 6 October of 2015 (C-362/14 - Schrems). 2015, C-362/14. http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=523715.

This important judgement declares that “Article 25, section 6, of Directive 95/46/CE of the European Parliament and of the Council, of 24 of October of 1995, On the protection of individuals with regard to the processing of personal data and on the free movement of such data, in version modified by Regulation (CE) n° 882/2003 of the European Parliament and of the Council, of 29 September 2003, understood in the light of articles 7, 8 and 47 of the Charter of Fundamental Rights of the European Union, must be interpreted as meaning that a decision adopted pursuant to that provision, such as Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46 on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, by which the European Commission finds that a third country ensures an adequate level of protection, does not prevent a supervisory authority of a Member State, within the meaning of Article 28 of that directive as amended, from examining the claim of a person concerning the protection of his rights and freedoms in regard to the processing of personal data relating to him which has been transferred from a Member State to that third country when that person contends that the law and practices in force in the third country do not ensure an adequate level of protection.

Definitely, the ECJ in the judgement of 6 October 2015 has declared that “Decision 2000/520 is invalid”.

7. European Commission (2016). “EU Commission and United States Agree on New Framework for Transatlantic Data Flows: EU-US Privacy Shield (IP/16/216).”
8. “Do Not Track” is a technology and policy proposal that allows to opt for no tracking on websites visited, including analysis services, publicity networks and social platforms. Currently, some websites offer a reliable tracking and allow for the activation of “no tracking” by means of tools for blocking, but they are not always easy to use or integral. Similar to the popular “Do Not Call registry”, the “Do Not Track” service prevents cybernauts from being followed and provides users with a simple and sustained option to opt for no tracking in third party websites.

9. Federal Trade Commission (2015). http://www.ftc.gov/.

10. Decision of the Constitutional Court 290/2000, of 30 November is a result of a series of recourses (201/1993, 226/1993 y 236/1993) lodged by the Executive Council of the Generalitat of Catalonia, the Ombudsman, the Parliament of Catalonia and 56 Members of Parliament against certain articles of Law 5/1992, of 29 October, Regulation of Automated Personal Data Processing. This decision includes pronouncements of enormous interest referring to the nature and functioning of the Data Protection Agency of the State, and also the recognition of a new fundamental right: “the right to freedom of information technology.”

11. One interesting project amongst others is a project for standardized icons created by https://disconnect.me/icons. As explained on their website, their mission is: “At Disconnect our mission is to make the Internet better by giving people greater transparency and control over the personal information they share online. We do what we do to make it easier for people to protect their privacy and enjoy the Internet”.

12. The “right to be forgotten” applied to search engines involves the erasure and blocking of contents in the results indices of internet searches. Following Decision C-131/12 of the Court of Justice of the EU Sentencia C-131/12 del Tribunal de Justicia de la UE, of 13 May 2014 in the case Google Spain, S.L., Google Inc. And the Spanish Data Protection Agency, it is considered that search engines carry out personal data processing and therefore that they have to assume the responsibilities that such processing implies. Thus, when they direct their services to European consumers, they must comply with the EU regulations in force and, as a consequence, attend to, study and resolve those requests to exercise the right to cancel and object to data treatment in cases in which the information has become obsolete and there is no public interest in accessing it.

The practical application of this decision requires that the search engines be able to find a balance between the rights of the data subject and a legitimate general public interest to access the information. This consideration will be based on four main factors: 1) the nature of said information in question, whether inexact or false, incomplete or inappropriate, excessive, obsolete or no longer relevant; 2) the sensitive nature of said information for the private life of an individual; 3) the public interest in disposing of this information at present; and 4) the role of said person in public life.

The request can therefore be sent directly to the controller of the search engine regardless of whether the data be eliminated or not from the website where they were published, and it is the search engine that will decide, case by case, about the validity of each individual request always taking into account the factors indicated previously. In the case of the user not being in agreement with the response from the search engine, they can seek advice at the data protection agency or in the courts of their jurisdiction so that their application, if legitimate, can be resolved successfully.

13. The European Parliament states that “The digital single market is one of the most promising and challenging areas of progress, creating potential efficiency gains of EUR 415 billion. It opens up new opportunities to boost the economy through
e-commerce, while at the same time facilitating administrative and financial compliance for businesses and empowering customers through e-government. Market and government services developed within the digital single market are evolving from fixed to mobile platforms and becoming increasingly ubiquitous, offering access to information and content anytime, anywhere and on any device (ubiquitous commerce and ubiquitous government). These advances call for a regulatory framework that is conducive to the development of cloud computing, borderless mobile data connectivity and simplified access to information and content, while safeguarding privacy, personal data, cybersecurity and net neutrality”.

The legal foundation for the digital single market is found in articles 4, section 2, letter a), 26, 27, 114 and 115 of the Treaty of the Functioning of the European Union (TFUE).

14. Article 56 of the GDPR regulates the competence of the lead supervisory authority and states that “Without prejudice to Article 55, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60.

15. Article 37 et seq. GDPR.

16. There are various studies on the issue. Some of the most important are the following: Paños Pérez, A. (2012); Rallo Lombarte, Artemi, & Díaz Díaz, E. (2014); Martínez Martínez, Ricard. (2014); Moya Izquierdo, Sara, and Isabela Crespo Vitorique. 2014.

17. SPEECH/11/183, Viviane Reding, Vice-President of the European Commission, EU Justice Commissioner, Your data, your rights: Safeguarding your privacy in a connected world, Privacy Platform "The Review of the EU Data Protection Framework", Brussels, 16 March 2011. http://europa.eu/rapid/press-release_SPEECH-11-183_en.htm?locale=en. “Peoples’ rights need to be built on four pillars: The first is the “right to be forgotten”: a comprehensive set of existing and new rules to better cope with privacy risks online. When modernizing the legislation, I want to explicitly clarify that people shall have the right – and not only the "possibility" – to withdraw their consent to data processing. The burden of proof should be on data controllers – those who process your personal data. They must prove that they need to keep the data rather than individuals having to prove that collecting their data is not necessary (...))”.

18. Comentario al Reglamento de Desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal (aprobado por RD 1720/2007, de 21 de diciembre). Estudios y Comentarios Legislativos (Civitas). Editorial Aranzadi, SA, Diciembre de 2008.

19. It is useful to clarify the difference between the right to cancellation and the right to object. In the words of the Spanish data protection agency, the AEPD, “The right to object is set out as a different right to the right to cancellation as the processing of the data referred to for cancellation cannot be considered as lawful, either because they are inappropriate or because they challenge the principles of quality as consecrated in article 4 of Organic Law 15/1999. However, the right to object operates in the case of the data processing being fully lawful, but because of a specific situation specified by the data subject, there is a request for the processing to be excluded. As a consequence, exercising the right to object obliges the controller of the files to carry out an assessment of the personal situation of the data subject, to consider whether said processing should be excluded.” (Informe Jurídico AEPD 0168/2012).

20. Comentario a la ley Orgánica de Protección de Datos de Carácter Personal. Estudios y Comentarios Legislativos (Civitas). Troncoso Reigada, A. Editorial Aranzadi, SA, June of 2010.

21. Resolución: R/00122/2015, Procedimiento N° PS/00524/2014, 9 February 2015.

22. Resolución AEPD R/00066/2003.
23. Judgement of the Court of Justice of the European Union (Grand Chamber), of 13 May of 2014 (C-131/12 - Google Spain v. Google), 2014, C-131/12.

24. For more information on the practical application and the criteria for considerations: Guidelines on the implementation of the Court of Justice of the European Union judgment on “Google Spain and inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja Gonzalez” c-131/121. WP225. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf.

Disclosure statement
The authors report no conflicts of interest. The authors alone are responsible for the content and writing of this article.

Note on contributor
Efren Diaz Diaz is a lawyer and Senior Associate at the law firm Bufete Mas y Calvet in Madrid, Spain. He is Consultant-Auditor of Information Systems, Head of the Department of Technology and Geospatial Law and a specialist in Civil Law and Administrative Litigation. He holds an International Master’s Degree in Data Protection, Transparency and Information Access (University of San Pablo CEU). He is currently the Spanish Lawyer in the IDEE Working Group in Spain and is an expert on the European Commission for ‘INSPIRE Maintenance and Implementation’ in the Infrastructure for Spatial Information in the European Community. He is a Corporate Member of the Centre for Spatial Law and Policy (U.S.A) and Spokesperson on the Technical Standardisation Committee AEN/CTN 148 for Digital Geographic Information in AENOR. He lectures on the Master’s Degree programme for Company and Fiscal Law and the Access to Law programme at the University of Navarra. He is a member of the Geovation Hub at the Ordnance Survey in London and is an investigator at the Open Data Institute (UK).

References
AEPD. 2007. Informe Juridico AEPD 1 August 2007.
Blume, P. 2012. "Will It Be a Better World? The Proposed EU Data Protection Regulation." International Data Privacy Law 2 (3): 130–36. doi:10.1093/idpl/ips007.
Council of the European Union. 2015. http://www.consilium.europa.eu/en/press/press-releases/ 2015/12/18-data-protection/http://ec.europa.eu/public_opinion/archives/ebs/ebs_431_en.pdf.
Court of Justice of the European Union. 2003. Judgement of the Court (Grand Chamber), of 6 November 2003 (C-101/01 - Bodil Lindqvist). 2003, C-101/01. http://curia.europa.eu/juris/ document/document.jsf?text=&docid =48382&pageIndex =0&doclang=ES&mode=lst&dir =&occ=first&part =1&cid =1129584.
Diaz Diaz, E. 2016. “Max Schrems: ‘El Escudo de Privacidad UE-EEUU Volverá Directamente a La Corte de Luxemburgo.” Lawyerpress.com. http://www.lawyerpress.com/news/2016_03/ 0103_16_001.html.
El Pais Digital. 2012. Viviane Reding: Quien pone datos personales en la Red tiene derecho a recuperarlos. Accessed 25 January 2012. http://www.madrimasd.org/informacionidi/noticias/noticia.asp?id =51316.
Europa Press. 2015. Google desiste en 136 casos sobre el ‘derecho al olvido’ recurridos ante la Audiencia Nacional. Accessed 23 January 2015. http://www.europapress.es/sociedad/noticia-google-desiste-136-casos-derecho-olvido-recurridos-audiencia-nacional-20150123193520.html.
European Commission. 2010a. “Communication from The Commission to The European Parliament, The Council, The Economic and Social Committee and The Committee of the
Regions "A comprehensive approach on personal data protection in the European Union." COM (2010) 609 final. Plan de acción de la Comisión por el que se aplica el Programa de Estocolmo - COM (2010) 171 final.

European Commission. 2010b. "Special Eurobarometer 359," Attitudes on Data Protection and Electronic Identity in the European Union. http://ec.europa.eu/public_opinion/archives/eb_special_359_340_en.htm.

European Commission. 2012a. “Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data.” General Data Protection Regulation. http://eur-lex.europa.eu/procedure/ES/2012_11?rid=1&qid=1443173807357.

European Commission. 2012b. Communication from The Commission to The European Parliament, The Council, The European Economic and Social Committee and The Committee of the Regions, Safeguarding Privacy in a Connected World, A European Data Protection Framework for the 21st Century. http://register.consilium.europa.eu/doc/srv?l=EN&f=ST5852 2012 INIT.

European Commission. 2012c. Conclusions of the Communication from The Commission to the European Parliament, The Council, The European Economic and Social Committee and The Committee of the Regions (COM 2012) 9 final, January 25, 2012.

European Commission. 2015. Special Eurobarometer 431. 'Data Protection.' DOI: 10.2838/552336. http://ec.europa.eu/public_opinion/archives/ebs/ebs_431_en.pdf.

European Commission. 2016. Reforma de La Protección de Datos: Nuevas Reglas Adaptadas a La Era Digital. http://www.europarl.europa.eu/news/es/news-room/20160407IPR21776/Reforma-de-la-protect%C3%B3n-de-datos-%E2%80%93-Nuevas-reglas-adaptadas-a-la-era-digital.

European Parliament and Council. 1995. Directive 95/46/CE of the European Parliament and of the Council of 24 October 1995, On the protection of individuals with regard to the processing of personal data and on the free movement of such data. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046.

European Parliament and Council. 2010. “The Charter of Fundamental Rights of the European Union.” CFRUE. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:en:PDF.

European Parliament and Council. 2016. “Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, On the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.” (General Data Protection Regulation). http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.SPA&toc=OJ:L:2016:119:TOC.

European Parliament. 2016. "The ubiquitous digital single market." Fact Sheets on the European Union. http://www.europarl.europa.eu/atyourservice/en/displayFtu.html?ftuId=FTU_5.9.4.html.

Fellmeth, A. X., and M. Horwitz. 2009. Guide to Latin in International Law. Oxford University Press.

International Conference of Data Protection and Privacy Commissioners. 2009. International Standards on the Protection of Personal Data and Privacy. https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Cooperation/Conference_int/09-11-05_Madrid_Int_standards_EN.pdf.

International Conference (35th) of Data Protection and Privacy. 2013. Resolution on Anchoring Data Protection and the Protection of Privacy in International Law. 24 September 2013. https://icdppc.org/wp-content/uploads/2015/02/International-law-resolution.pdf; http://www.boe.es/buscar/doc.php?id=DOUE-Z-2010-70003.

Martínez Martínez, Ricard. 2014. “Aplicar el derecho al olvido.” Revista Aranzadi de derecho y nuevas tecnologías. Editorial Aranzadi. https://dialnet.unirioja.es/servlet/articulo?codigo=4917063.
Moya Izquierdo, Sara, and Isabela Crespo Vitorique. 2014. “Los motores de búsqueda y el ‘derecho al olvido’ cuando la tecnología avanza más rápido que el Derecho.” Unión Europea Aranzadi. Editorial Aranzadi. https://dialnet.unirioja.es/servlet/articulo?codigo=5052233&info=resumen&idioma=ENG.

Official Journal of the European Communities. 1995. n° L 281 de 23/11/1995. Pages 0031–0050. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:1995:281:FULL&from=EN.

Paños Pérez, A. 2012. Conflict between freedoms of expression and information and the right of honour, privacy and self-image of minors. Revista de Derecho. Facultad de Ciencias Jurídicas y Sociales. https://dialnet.unirioja.es/servlet/articulo?codigo=5333364&info=resumen&idioma=ENG.

Piñar Mañas, J.L. 2008a. ¿Existe la privacidad?, 19. Madrid: Universidad CEU San Pablo.

Piñar Mañas, J.L. 2008b. ¿Existe la privacidad?, 26–27. Madrid: Universidad CEU San Pablo.

Piñar Mañas, J. L., and A. Canales Gil. 2008. Legislación de protección de datos, 91. Madrid: Iustel.

Rallo Lombarte, Artemi, and Díaz Díaz, E. 2014. “Caso Google vs. España: Sentencia Del TJUE 13 de Mayo de 2014.” Actualidad Jurídica Aranzadi, no. 886: 8.

United Nations. 1995. “Resolution 45/95 of the General Assembly of the United Nations, 14 of December 1990.” Guidelines for the Regulation of Computerized Personal Data Files. United Nations. http://inicio.ifai.org.mx/DocumentosdeInteres/D.3BIS-cp-Directrices-de-Proteccion-de-Datos-de-la-ONU.pdf.

United States and White House Office. 2012. “Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy.” Washington DC: The White House. http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

Warren, S. D., and L. D. Brandeis. 1890. "Right to Privacy." Harvard Law Review 4 (5): 193–220. http://www.jstor.org/stable/1321160.

The White House. 2012. "We Can’t Wait: Obama Administration Unveils Blueprint for a ‘Privacy Bill of Rights’ to Protect Consumers Online." Washington DC: Office of the Press Secretary. https://www.whitehouse.gov/the-press-office/2012/02/23/we-can-t-wait-obama-administration-unveils-blueprint-privacy-bill-rights.

The White House. 2016. Executive Order: Establishment of the Federal Privacy Council. Executive Orders. https://www.whitehouse.gov/the-press-office/2016/02/09/executive-order-establishment-federal-privacy-council.