UNIVERSITÀ POLITECNICA DELLE MARCHE
FACOLTÀ DI ECONOMIA "GIORGIO FUÀ"

Corso di Laurea Magistrale in International Economics and Commerce

PERSONAL DATA PROTECTION IN EUROPE

The impact of the GDPR on the Italian company TOD'S S.p.A.

LA PROTEZIONE DEI DATI PERSONALI IN EUROPA

L'impatto del GDPR sull'azienda italiana TOD'S S.p.A.

Relatore: Chiar.mo
Prof. Giancarlo Vilella

Tesi di Laurea di:
Matteo Magnanelli

Anno Accademico 2021/2022

TABLE OF CONTENTS

ABSTRACT……6

INTRODUCTION……..9

CHAPTER 1: SHAPING EUROPE'S DIGITAL FUTURE……12

1.1 The Three Pillars For The Digital Europe Of The Future……..12

1.1.1 Technology That Works For People……...13

1.1.2 A Fair And Competitive Economy…….17

1.1.3 An Open, Democratic And Sustainable Society…….19

1.2 Building Europe's digital sovereignty……...22

1.2.1 Cyber Security……24

1.2.2 Digital infrastructure upgrading…….27

1.2.3 Data protection……...30

CHAPTER 2: THE AGE OF DATA……...33

2.1 A World Full Of Data……33

2.2 Big Data……35

2.3 Benefits achievable from the use of big data…….38

2.4 Abuse of Data: Cambridge Analytica……...39

CHAPTER 3: EVOLUTION OF DATA PROTECTION IN EUROPE…….44

3.1 The birth of the concept of privacy……44

3.2 Europe as main promoter of the right to privacy: Art. 8 ECHR…….47

3.3 The term "privacy," electronic database resolutions, and "data protection"……..50

3.4 Convention 108, 1981……...52

3.4.1 The content of Convention 108……..54

3.4.2 The objectives of Convention 108……..55

3.4.3 The principles of Convention 108……..56

3.5 Steps toward the creation of European data protection legislation……60

3.6 Directive 95/46/EC……...64

3.6.1 The objectives of the Directive……...66

3.6.2 The content of the Directive……...67

3.6.3 The principles, consent and sensitive data of the Directive….69

3.7 Impact of the Directive on national disciplines: focus on Italy……..72

3.8 Other acts before the General Data Protection Regulation of 2016……74

CHAPTER 4: THE GENERAL DATA PROTECTION REGULATION…...82

4.1 The adoption of Regulation (EU) 2016/679……..82

4.1.1 The objectives of the Regulation……..83

4.1.2 Material scope and territorial scope……..85

4.1.3 Definitions……...87

4.2 The principles of the Regulation……...89

4.3 Rights of the data subject……...92

4.3.1 Right to erasure (“right to be forgotten”)……94

4.3.2 Right to data portability……..97

4.4 Data controller and processor……98

4.4.1 Records of processing activities……...102

4.4.2 Privacy by design and by default……..104

4.4.3 Security of processing and data breach……105

4.4.4 Data protection impact assessment and prior consultation...108

4.4.5 Data protection officer……..111

4.4.6 Codes of conduct and certification……...114

4.5 Transfers of personal data to third countries or international organisations……116

4.6 Independent supervisory authorities……...117

4.7 The tightening of the liability and penalty system……...119

CHAPTER 5: IMPACT OF THE GDPR ON THE ITALIAN COMPANY TOD'S S.P.A……...123

5.1 Introduction……123

5.2 TOD’S S.p.A……...124

5.3 GDPR compliance process……..129

5.4 Data Protection Officer……...134

5.5 Drafting of data protection documents……142

5.6 Is the GDPR still relevant today? ……148

CONCLUSION……...151

BYBLIOGRAPHY ……155

SITOGRAPHY……...158

ABSTRACT

La presente tesi si pone l'obiettivo di approfondire come l'Unione Europea ha gestito e gestisce tutt'ora la protezione dei dati personali.

I cinque capitoli di cui si compone l'elaborato cercheranno di esaminare la tematica sotto differenti punti di vista per avere una visione completa e dettagliata dei maggiori aspetti che riguardano questo argomento così attuale e rilevante.

Il primo capitolo va a definire quali sono i tre pilastri su cui si vuole investire per dare forma all'Europa digitale del futuro: un'Europa che ambisce ad essere aperta, democratica e sostenibile con un'economia equa e competitiva nel mondo la cui tecnologia sia a servizio dei suoi cittadini. Per fare ciò è fondamentale che l'Unione raggiunga una maggiore sovranità digitale per rendersi indipendente dalle altre superpotenze e preservare la propria capacità di agire in un mondo sempre più globalizzato. È qui che si inserisce l'importanza di proteggere i dati dei cittadini, delle imprese e delle istituzioni europee.

Nel secondo capitolo si va ad indagare sul perché i dati e soprattutto i big data sono così importanti nel mondo moderno. Cosa sono i dati? Che benefici si possono ottenere dalla loro raccolta e elaborazione? E cosa può accadere se finiscono nelle mani sbagliate e vengono usati per fini impropri? La rivoluzione digitale e le nuove tecnologie stanno generando una vera e propria esplosione dei dati ed è importante essere consapevoli dei rischi e dei grandi vantaggi che questi possono portare se

usati in maniera corretta.

Nel terzo capitolo si entra nel vivo dell'evoluzione della protezione dei dati personali in Europa. Partendo dalla nascita del concetto di privacy si vanno a definire tutti i passaggi e le regolamentazioni più importanti che hanno contraddistinto questo processo. Si analizzerà l'articolo 8 della CEDU, la convenzione 108 del 1981, la Direttiva 95/46/CE fino ad arrivare al Regolamento UE n. 2016/679.

Il quarto capitolo si concentrerà solo ed esclusivamente all'analisi di questo ultimo rivoluzionario strumento, meglio conosciuto come GDPR (Regolamento generale sulla protezione dei dati), che vuole offrire una stabilità giuridica alla disciplina sulla protezione dei dati personali all'interno del territorio comunitario, conferendo alle imprese europee maggiore competitività sul mercato internazionale e allo stesso tempo ottenere maggiore fiducia dai consumatori finali. Verranno analizzate le figure introdotte dal Regolamento EU del titolare del trattamento e responsabile del trattamento, definendo i loro doveri affinché i diritti dell'interessato vengano soddisfatti. Verranno definiti gli obiettivi, i principi introdotti volti ad una tutela preventiva e precauzionale piuttosto che successiva-riparatoria.

Infine l'ultimo capitolo analizza il caso reale dell'azienda italiana TOD'S S.p.A. specializzata nella produzione di calzature, abbigliamento e accessori di lusso. Grazie a dei colloqui con il Data Protection Officer del Gruppo è stato possibile comprendere che impatto ha avuto il GDPR sull'azienda e come questa si è dovuta

adeguare alla nuova normativa. Si è compresa meglio l'importanza della figura del DPO all'interno dell'azienda e per concludere ci si è interrogati se il Regolamento, a distanza di qualche anno dalla sua entrata in vigore, è ancora efficace ed attuale.

INTRODUCTION

Data is considered the oil of the 21st century.

Recent years have seen exponential growth in data creation and processing, and this trend is not going to stop anytime soon. As a result, it is critical that there are regulations in place to protect data so that citizens can feel protected and free to move in an increasingly digitized world.

The purpose of this thesis is to delve into this very timely and fundamental topic by analyzing how the European Union has handled and still handles the protection of personal data.

The five chapters of which the paper is composed will try to examine the subject from different points of view in order to have a complete and detailed vision of the major aspects concerning the protection of personal data in Europe.

The first chapter aims to define what are the three pillars on which it is intended to invest to shape the digital Europe of the future: a Europe that aspires to be open, democratic and sustainable with a fair and competitive economy worldwide whose technology is at the service of its citizens. To do this, it is essential that the Union achieve greater digital sovereignty to make itself independent of other superpowers and preserve its ability to act in an increasingly globalized world. This is where the importance of protecting the data of European citizens, businesses and institutions comes in.

The second chapter goes on to investigate why data and especially big data are so important in the modern world. What is data? What benefits can be gained from their collection and processing? And what can happen if it gets into the wrong hands and is used for improper purposes? The digital revolution and new technologies are generating such an explosion of data, and it is important to be aware of the risks as well as the great benefits it can bring if used properly.

Chapter three gets to the heart of the evolution of personal data protection in Europe. Starting from the birth of the concept of privacy, all the most important steps and regulations that have marked this process will be defined. It will analyze Article 8 of the ECHR, Convention 108 of 1981, Directive 95/46/EC up to EU Regulation No. 2016/679.

The fourth chapter will focus solely and exclusively on the analysis of this latest revolutionary instrument, better known as GDPR (General Data Protection Regulation), which aims to provide legal stability to the discipline of personal data protection within the EU territory, giving European companies greater competitiveness on the international market and at the same time gaining more trust from end consumers. The figures introduced by the EU Regulation of the data controller and data processor will be analysed, defining their duties so that the rights of the data subject are met. The objectives, principles introduced aimed at preventive and precautionary rather than subsequent-remedial protection will be defined.

Finally, the last chapter analyses the real case of the Italian company TOD'S S.p.A. specializing in the production of luxury footwear, clothing and accessories. Thanks to interviews with the Group's Data Protection Officer, it was possible to understand what impact the GDPR had on the company and how it had to adapt to the new legislation. A better understanding was gained of the importance of the figure of the DPO within the company, and to conclude, questions were raised as to whether the Regulation, a few years after it came into force, is still effective and up to date. Compliance with European regulations, and in particular with the GDPR, should therefore not be seen as mere bureaucratic accomplishment but as a key investment for the future in order to be able to meet the challenges of the international market and emerging technologies. The EU Regulation is a necessary response to protect the personal data of European citizens and contribute to the common welfare.

Chapter 1

SHAPING EUROPE'S DIGITAL FUTURE

1.1 THE THREE PILLARS FOR THE DIGITAL EUROPE OF THE FUTURE

With the rise of new digital technologies, human life has changed profoundly.

Daily life, the way of working and doing business, the way of travelling, learning, communicating and relating has been completely overturned and, more and more frequently, new methods of digital communication are invented, new social media, revolutionary digital enterprises are opened which transform our world. All this is generating an amount of data that is increasing exponentially year after year and if we could pool this collected information, process it and exploit it for noble purposes, everyone could benefit and the value creation that would occur would lead to great advantages and successes.

In the idea of the European Commission, this digital transformation should enrich the lives of all citizens and the choices that will be made now will be fundamental to shaping the future of digital Europe[1]. In fact, the Commission and its President

[1] European Commission, 19.2.2020, Brussels, "*Shaping Europe's digital future*", communication from the commission to the european parliament, the council, the european economic and social committee and the committee of the regions.

Ursula von der Leyen, have decided to include the digital strategy among the 6 priorities for the five-year period 2019 - 2024[2] together with the European Green Deal[3], an economy that works for people, a stronger Europe in the world, promotion of the European lifestyle and a new push for European democracy. As the President stressed, these 6 goals are closely interconnected and the new digital world will help to achieve the other priorities by promoting for example a greener and sustainable economy and decrease inequalities among European citizens.

This new digital Europe that will be created should reflect the values of the best part of the Union: open, fair, diverse, democratic and confident. In order to achieve this and to increase the well-being of citizens, 3 pillars have been stipulated on which to base the next actions.

The three pillars are: technology that works for people, a fair and competitive economy, and an open, democratic and sustainable society.

1.1.1 Technology that works for people

Europe is stronger when it acts together and joins forces between its member states and the EU. Europe needs to share its investments in research and innovation, exchange experiences and cooperate across countries, involving regions and municipalities, academia, civil society, financial institutions and social enterprises.

[2] Von Der Leyen U., 2019, "*A Union that strives for more. My agenda for Europe*"
[3] European Commission, 11.12.2019, Brussels, *"The European Green Deal"*

Only in this way will it be possible to have a real development that will lead to the diffusion and adoption of technologies that make a real difference in people's daily lives; it will be possible to build a strong and competitive economy that masters and shapes technology in a way that respects European values.

Europe must invest more in the strategic capabilities that enable the development and utilization of digital solutions at scale and fight for the operability of key digital infrastructure, such as extensive 5G networks powered by secure fiber (and future 6G) and deep tech.

Connectivity is the fundamental element of digital transformation.

It is what allows data to flow, people to collaborate wherever they are, and connects more objects to the Internet, transforming manufacturing, mobility, and logistics chains. Investing in connectivity is vital if we want to harness Europe's digital growth potential. This requires adequate investment at European, national and regional levels.

The EU's new Multiannual Financial Framework will contribute to these objectives with targeted funding programmes and by making use of the InvestEU Guarantee[4] and Structural and Rural Development Funds. This public funding must be used to stimulate private investment, because only if there is a wide range of private and

[4] D'Alfonso A., 2021, *"InvestEU programme. The EU's new investment support scheme",* EPRS European Parliamentary Research Service

public capital available to finance digital innovation will it be possible to close investment gaps.

In addition to investing in connectivity, Europe needs to invest in deep technology, human capital, as well as smart energy and transportation infrastructure. According to a study conducted by the European Commission with the McKinsey Global Institute, part of the world's leading multinational strategy consulting firm, implementing reforms and increasing investment in research and development and technology advancement could produce 14% additional cumulative GDP growth by 2030[5]. This would obviously create many jobs, and this is a socio-economic boost that the Union cannot afford to lose.

However, investing in innovation is only part of the story. A true digital transformation must start with European citizens and businesses being able to trust that their applications and products are secure. To address this growing threat, we need to establish consistent rules for businesses and more secure mechanisms for proactive information sharing; we need to have laws in place to defend cybersecurity; and we need to ensure that law enforcement and judicial authorities can work effectively with the right tools to use against cybercriminals. Additionally, it is crucial to raise awareness of cybersecurity among EU citizens and make sure

[5] McKinsey Global Institute, 2020, *"Shaping the digital transformation*", Study conducted for the European Commission.

they can trust the technology itself, as well as the way it is used. This is especially important when it comes to artificial intelligence. In this regard, the European Commission is presenting a white paper on creating ecosystems of excellence that sets out options for a legislative framework for trusted AI with a follow-up on security, accountability, fundamental rights, and data.

Improving education and skills is another key part of the overall vision for digital transformation in Europe. European companies need digitally skilled employees to thrive in the global marketplace, and in turn, workers need digital skills to succeed in an increasingly digitized labour market. More women can and should have rewarding careers in technology.

The need for digital skills however also permeates our personal lives therefore having a minimum level of literacy and basic digital skills has become a prerequisite to participate effectively in today's society.

Lastly, new challenges are also emerging in terms of online working conditions. There are often few or no legal protections in the various online platforms and to address this issue the Commission will therefore propose a strengthened framework for platform workers.

1.1.2 A fair and competitive economy

In a world where technology is gaining in importance, Europe must continue to act and decide independently and reduce over-reliance on digital solutions created elsewhere.

For the development of many products and services, data must be widely and easily available and simple to use and process. Data has become a key factor in production and, for this reason, we need to build a true single European market for data based on European rules and values. This is all part of the European data strategy that will seek to make Europe a world leader in the agile data economy[6].

Many European companies and particularly SMEs (a vital part of the European economy) have been slow to adopt digital solutions and have missed opportunities to grow. The Commission will seek to facilitate the transition to a more digital, clean, circular and competitive European industry by increasing access to finance and markets. To do this, it is also important to have a frictionless single market with clear and proportionate rules that are uniformly applied across the EU, unhampered by local or national regulations that increase administrative burdens for small businesses in particular.

To create a fair economy, it is important that rules that apply offline, such as competition, consumer protection, intellectual property, taxation and workers'

[6] European Commission, 19.2.2020, Brussels, *"A European strategy for data"*

rights, should also apply online. Consumers, especially the most vulnerable, need to be able to trust digital products and services even if they come from outside the EU.

With regard to EU competition law, for example, it is important that its fundamentals are as relevant for traditional industries as for digital ones. The Commission is reflecting on the effectiveness of the way in which the current rules are applied, for example in relation to antitrust remedies, and is also conducting an assessment and review of the rules themselves to ensure that they respond to today's digital challenges.

Other key issues for Europe's digital future include access to data, pooling and sharing, and the balance between online and offline commerce. However, competition policy alone cannot address all the systemic problems that can arise in the platform economy. Additional rules will be needed to ensure contestability, fairness, and innovation and market entry opportunities, as well as public interests beyond competition or economic considerations.

Ensuring fairness in the digital economy is a challenge. In today's digital world, a few giant companies make the majority of the profits on the value that is created in a data-driven economy. These profits are often not taxed because of outdated tax rules that distort competition. This is why the Commission will be looking to address the tax challenges of digitizing the economy.

1.1.3 An open, democratic and sustainable society

European values, ethical rules, and social and environmental standards must also apply in the digital space. Citizens are entitled to technology they can trust, and what is illegal offline must also be illegal online.

In recent years, Europe has led the way toward an open, fair, inclusive, and people-centric Internet with its General Data Protection Regulation, which sets standards and rules for platform-to-business cooperation. In order to protect European democracies with its values and its citizens, the Commission will continue to develop and implement innovative and proportionate rules for a digital society that is trustworthy, inclusive, fair and accessible to all.

What we want to achieve is that the digital world is as regulated as the offline one so that there are specific rules for services offered on the web and that the goods sold are not dangerous or counterfeit. In order for consumers to trust the online world it is also important that they have control over their data and identities and therefore that there are clearer rules on transparency, behavior and accountability of those who act as guardians of information and data flows.

People should also be able to control their online identity when authentication is required to access certain services on the web. A universally accepted public electronic identity (eID) is necessary for consumers to access their data and securely use the products and services they want.

In a world where much of the public debate and political advertising has shifted online, we must also be prepared to act to vigorously defend our democracies. Europe needs more transparency about the ways in which information is shared and managed on the internet so that we can avoid disinformation campaigns and stop fake news. For this reason, the Commission will present a European Action Plan for Democracy and a specific action plan for the media and audiovisual sector.

The digital component will also be key to achieving the ambitions of the European Green Deal and sustainable development goals by advancing the circular economy and reducing the carbon footprint. For example, key sectors such as precision agriculture, transport and energy can benefit immensely from the digital solutions that are being and will be developed, and thanks to the data collected it will be possible to increase energy efficiency by understanding where less fossil fuels and more renewables can be used.

The ICT (Information Communication Technology) sector also needs to undergo its own green transformation. The sector's environmental footprint is significant, estimated at 5-9% of total worldwide electricity use and more than 2% of all emissions[7]. Data centers and telecommunications will need to become more energy

[7] Bughin J., Hazan E., Manyika J., 2019, *"Tech for Good. Smoothing disruption, improving well-being"*

efficient, reuse waste energy and use more renewable energy sources. They can and must become climate neutral by 2030[8].

The power of data is also essential in healthcare. Digitized medical records, collected in a European health data space, can lead to better treatment for major chronic conditions, including cancer and rare diseases, but also to equal access to high-quality health services for all citizens.

Following these three pillars the Commission will try to give the best possible shape to the future of digital Europe and if we proceed as planned, the European model can be an inspiration to many other partners around the world. The European Union is already seen by many as a region that is very open to trade and investment as long as anyone who comes to do business in its territory accepts and respects its rules, and this is how it should continue to be. In addition, the Commission is committed to continuing to work closely with its international partners, such as the United Nations, OECD, ISO, G7 and G20, to find common approaches to developing international digital norms and standards.

During this revolution, it should never be forgotten that technologies are just a tool and this tool must be used to improve the well-being of all citizens, not just a few more privileged ones but all, always remembering the respect and inclusion.

[8] Vitali Roscini A., Rapf O., Kockat J., 2020, *"On the way to a climate-neutral Europe",* BPIE

However, in order for this great change to truly succeed, Europe must be able to choose and pursue digital transformation in its own way. European citizens, companies, governments and institutions must be able to develop and deploy their key capabilities without external pressure, thereby reducing their dependence on other parts of the world that currently dominate the global stage. If Europe truly wants to become a world leader in this area, it will first have to work on its digital sovereignty.

1.2 BUILDING EUROPE'S DIGITAL SOVEREIGNTY

The European Council on Foreign Relations (ECFR) defines digital sovereignty as a country's ability to control new digital technologies and their effects on society, preserving for itself the capacity to act in the world, even while remaining deeply interdependent.

The European Union has long been advocating a strategy to assert its digital sovereignty, although the debate has only recently become much more intense. Indeed, especially in the last few years, there is growing concern that EU citizens, businesses, and member states are gradually losing control over their data, their ability to innovate, and their power to shape and enforce legislation in the digital environment. The Covid-19 pandemic that struck the EU in the spring of 2020 showed how dramatically societies are dependent on data, network stability, and digitization more generally, and there has thus been a strong reinforcement of the

view that there is an urgent need to achieve strategic autonomy in developing digital solutions in line with the founding principles and values of the Union[9].

Rising tensions between the United States and China are an additional incentive for Europe to develop its digital sovereignty. The two superpowers are increasingly serving their narrow interests without looking at the needs of other international players, and Europe risks becoming just a bystander that does not keep up with the times if it does not gain its own independence. The EU cannot continue to rely only on its own regulatory power but must become a technological power in its own right, and this it can only do with the cooperation of all member states. Referees do not win the game, and the EU can become the example of a digital sovereignty that protects democratic governments and ethical development, an alternative to the approaches of the United States and China.

Moreover, in today's world when we talk about big technology players, we cannot think only of nation-states such as the United States or China, but must also take into account technology companies that are now so rich and powerful that even states often cannot control them and impose rules on them that must be respected. Multinational corporations such as those encapsulated under the acronym GAFAM (Google, Apple, Facebook, Amazon, Microsoft), have become so powerful and large that there is almost no option other than what they offer. This leading role of

[9] Galvin J., LaBerge L., Williams E., 2021, "*The new digital edge: Rethinking strategy for the postpandemic era*", McKinsey Global Institute

them has often resulted in abuse of dominance and has led in several cases to problems of tax evasion, intrusion into their users' private lives, and violation of their privacy.

This strong external influence is increasingly bringing concern to EU policymakers who would like to curb this dependence on foreign technologies and services and seek to redistribute the wealth produced in the digital field by countering the current dangerous concentrations of wealth and power in the hands of a few oligopolistic companies.

If the EU really wants to seek to achieve its own digital sovereignty based on European values, it needs to update and adapt a number of its legal, regulatory and financial instruments, and to more actively promote European values and principles in areas such as cybersecurity, enhancing secure digital infrastructure and data protection.

1.2.1 Cyber security

Knowing how to protect computers, servers, networks and any electronic system from malicious cyber attacks is crucial to being independent and creating a secure and reliable environment.

According to a report carried out by Clusit (Italian Association for Information Security), 2,049 serious cyber attacks were recorded in 2021, an increase of nearly 10 percent over the previous year, for a monthly average of 171 attacks, the highest

figure ever recorded[10]. Cyber criminals have also taken advantage of the coronavirus pandemic to target sensitive data more heavily, and there is growing concern that, given the current conflict between Russia and Ukraine, there may be cyber attacks on countries hostile to the government in Moscow.

Already during the last 2014-2019 term, when the president of the European Commission was Jean-Claude Juncker, several measures were taken to address cyber-attacks. The 2016 Network and Information Security (NIS) Directive improved member states' cybersecurity capabilities and cooperation and mandated measures for companies to prevent and report security incidents and cyber-attacks in key sectors such as energy, transportation, banking, financial market infrastructure, the healthcare sector, drinking water supply and distribution, and digital infrastructure. The European Cybersecurity Act passed in 2018 created an EU-wide (non-mandatory) cybersecurity certification system for ICT products to ensure that consumers and businesses were protected from cybersecurity threats. As a result, the EU has begun to establish itself as a standard-setter in cybersecurity as non-EU countries, as well as private companies doing business in the EU, have updated their cybersecurity practices and policies to ensure compliance with these new and growing legal requirements.

[10] Clusit, 2020, *"Rapporto Clusit edizione marzo 2022"*

However, this is not always enough especially in a field that is evolving faster and faster, and in order to maintain sovereignty, one must continuously update.

Three main areas in the field of cybersecurity have been identified where action needs to be taken[11]:

- By 2023, the cybersecurity certification system, which provides a harmonized set of rules to ensure consumer and business protection, must be revised. An EU-wide mandatory (not just voluntary) certification scheme needs to be established to ensure a truly secure environment, especially for 5G networks.
- Second, insufficient coordination on cybersecurity has been identified as one of the main issues that EU policymakers need to address. In 2021, the European Commission unveiled plans for a joint cyberspace unit, a new platform that aims to strengthen cooperation between EU institutions and agencies and national authorities in member states. The joint cyberspace unit will provide a virtual and physical European platform for cooperation that will assist in countering large-scale cyber attacks.

Also in 2021, the regulation establishing the European Center of Expertise for Cybersecurity in Industry, Technology and Research and the Network of National Coordination Centers entered into force; the Commission has begun working with Romanian authorities on setting up the Center in Bucharest.

[11] European Commission, 2017, *"EU cybersecurity initiatives. Working towards a more secure online environment"*

- Finally, the cybersecurity threat has prompted a reflection on supply conditions in the EU. Certain security requirements (including, of course, cybersecurity) must become a mandatory aspect in all public procurement procedures for relevant infrastructure at both the EU and national levels. This is also why there are plans to revise the Network and Information Systems Security Directive (NIS 2 Directive) to harmonize the protection of the EU's critical digital sector and to finalize the adoption of an international procurement instrument to ensure mutual market access in public procurement. In addition, the ECA's proposal to establish a common procurement framework for cybersecurity infrastructure in the EU should be explored.

1.2.2 Digital infrastructure upgrading

The European Parliament has expressed concern about dependence on Chinese 5G infrastructure and Chinese technology companies such as Huawei and Zte, and more generally, concerns about growing European reliance on individual suppliers of essential components[12]. This overdependence increases exposure to potential supply disruption and creates a security risk. For this reason, Europe must seek to differentiate sources of supply and, to the extent possible, increase production of some IT components even within its own borders.

[12] Hobbs C., 2020, *"Europe's digital sovereignty: from rulemaker to superpower in the age of us-china rivalry"*

Another example of Europe's strategic dependence on foreign digital infrastructure is that of Cloud technology. Indeed, member states have little control over the data produced in the Union because it is generally stored under U.S. jurisdiction. This inevitably exposes citizens, businesses and public authorities to the conflicts that can potentially arise with foreign jurisdictions. European governments have therefore begun to move away from cloud solutions offered by non-European companies and instead employ cloud solutions designed within the Union. Of all the initiatives the one that is impossible not to mention is the ambitious Gaia-X, the new European cloud. First unveiled at the Digital Summit 2019 in Dortmund, Gaia X is a project that aims to build an infrastructure, the purpose of which is to achieve European digital sovereignty in the cloud. Gaia X will provide a single standard, shared among all partner countries, to ensure the security of EU countries' data, linking different cloud services together, resulting in an efficient, secure and competitive federation of data infrastructures and service providers across the EU[13]. In addition to the Cloud space, another point of fundamental importance to remain independent and compete in the international arena is artificial intelligence. In AI, the EU lags behind the U.S. and China in terms of private investment, and the level of adoption of AI technologies by companies and the general public is relatively low compared to the U.S. In order to make sure that we have a fairly advanced AI

[13] Eggers G, Fondermann B., 2020, *"GAIA-X: Technical Architecture",* Federal Ministry for Economic Affairs and Energy (BMWi)

system, it is crucial that the infrastructure to support it is also up to date. These are systems that need, at their base, powerful, reliable, scalable performant infrastructures, even more when considering the next evolutions of Artificial Intelligence that will be based on analytical processes and workloads that are non-traditional, data-intensive, and much more extensive than those we were used to managing. In today's technological landscape, most Artificial Intelligence algorithms need huge amounts of data and computing power to work. Here then, Europe needs to focus on the three main technological components of AI:

- The network infrastructure (and connectivity). These technology components are put under extreme pressure by the processes generated by AI, which is why it is necessary to work on their scalability, i.e., the ability to increase the size and volume of data circulating without a proportional use of resources and without having to change the core features.
- Server infrastructure. Meaning in this sense as a high processing capacity. Needed are nanotechnologies such as neuromorphic chips or GPUs so powerful that they can handle even heavy loads like those of Deep Learning algorithms.
- Storage. The area of storage in support of AI is perhaps the most critical area where we will see technologies mature hand in hand with AI itself, somewhat as has happened with infrastructure to support Big Data and is happening with IoT (Internet of Things).

1.2.3 Data protection

It is precisely in this context that the issue of personal data protection comes into play. There is growing concern among EU member states about lack of control over the data produced on their territory. As mentioned, the global public cloud market is now largely dominated by U.S. and Asian companies, and European governments and industry players have become concerned about using non-European data services since their legislation does not protect users to the same standards that would be held in Europe.

Technology companies are collecting huge amounts of personal data and sometimes this is being exploited in ways that are not totally lawful. The Cambridge Analytica scandal has shown how online platforms are also able to mine personal data for political profiling purposes. These trends ultimately result in European citizens gradually losing control over their personal information and losing trust in the technologies and those who manage them.

The European Union has already taken several measures to enhance its digital sovereignty with regard to data protection. The most important of these is certainly the General Data Protection Regulation (GDPR) passed in 2016 and also the introduction of the "right to be forgotten." In addition, the Commission has set out a European data strategy to promote international standards of protection.

The EU is seen as a standard-setter in privacy and data protection, with several countries incorporating GDPR provisions into their national legislation and some multinational companies choosing to adopt GDPR as a global operating standard.

To preserve this role at the international level, the Union must always update the legislative framework by monitoring the impact of emerging technologies and figuring out how to increasingly protect citizens while still respecting the founding values. For example, discussions are underway to give more guidelines for data protection in areas such as health and financial services and to see how to adapt the General Data Protection Regulation also adapting it to an environment increasingly pervaded by artificial intelligence.

The two most important and recent regulations that will take effect in 2023, two years after the first draft, are the Digital Markets Act (DMA) and the Digital Services Act (DSA).

The DMA was created to counter abuse of dominance before infringement occurs while the DSA aims to contribute to the proper functioning of the internal market for intermediary services by establishing harmonized rules for a safe, predictable, and reliable online environment.

Throughout this paper we will try to explore this macrotopic that is so contemporary and so sensitive in order to understand what the European Union has actually done

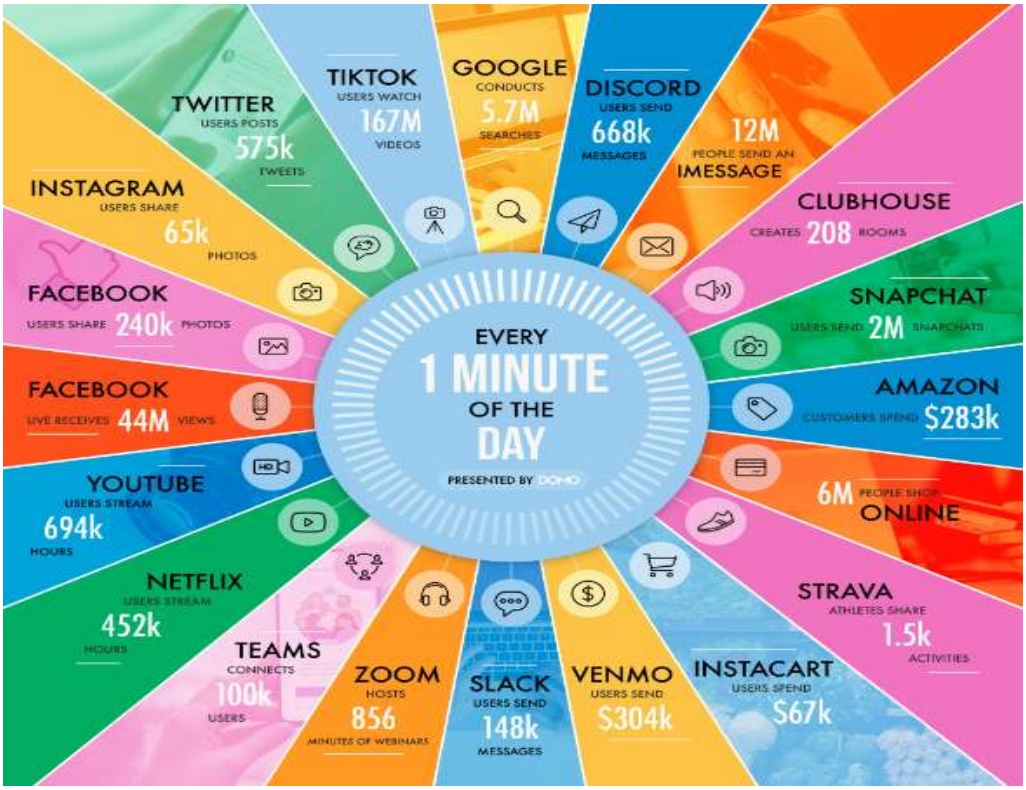
and is still doing to protect its citizens and their digital data. After further clarifying what is meant by data, we will see why it is so important in modern society and how it can be ethically harnessed knowing how to collect, analyze, and process it. We will look at the history and how it came to the current regulations by understanding how citizens, companies and governments had to adapt to reach the security standards decided at the European level. Finally, we will analyze what measures, urgent and less urgent, need to be taken in order to have a legislation in the future that is always efficient, up-to-date and functional; citizens can have confidence and can take advantage of new technologies with peace of mind and awareness, knowing that their data will be protected.

Chapter 2

THE AGE OF DATA

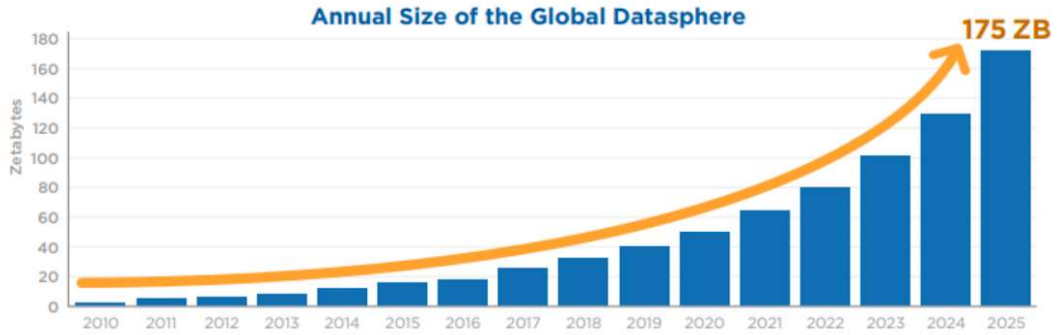
2.1 A WORLD FULL OF DATA

According to a research conducted by Domo, a company specialized in business intelligence and data visualization, every 60 seconds customers spend 283 thousand dollars on Amazon, 240 thousand photos are shared on Facebook, and every minute on Netflix users stream 452 thousand hours of video. Every 60 seconds, 5.7 million searches are conducted on Google.



Domo. *"Data Never Sleeps 9.0"*

The digital revolution and new technologies are generating an explosion of data, and year after year there is more than exponential growth. According to IDC (International Data Corporation), a company which specializes in market research and consulting, in just 3 years in 2025 , there will be 175 Zettabytes of data (1 Zettabyte corresponds to 10^21 bytes), more than double the amount of data currently held, about 80 ZB.



IDC, *"Global datasphere growth from 2010 to 2025"*

Data are generated through any medium: from sensors for gathering climate information to social media posts, via digital videos and images, GPS data collected through smartphones and tablets, transcription of purchase transactions, and many more.

All this information, if one is able to analyze it, can be turned into knowledge that would bring a clear source of competitive advantage and differentiation to companies that know how to exploit these data. At the same time, if this data gets

into the wrong hands or is used for illicit purposes, it can create great damage with disastrous consequences that are difficult to repair.

2.2 BIG DATA

When people refer to large aggregations of data that cannot be processed or analyzed by traditional analytical processes and tools, they are referring to Big Data. Although there is no single definition within which the concept of big data is encapsulated, scholars agree on a model consisting of the 3 elements introduced by Laney in 2001 plus 2 added more recently, called the "5V" model. Each V encloses an essential aspect that an analyzed dataset must have to be called "big." These are: Volume, Velocity, Variety, Veracity and Value[14].

- Volume.

This is the "V" that was originally referred to when talking about big data in early articles since the main focus was initially on size for storing information. The volume of data is constantly growing, and over the years there have been mainly two key factors that have contributed to the exponential increase in the volume of data collected and exploited. The first factor is the reduced cost of collecting, storing, processing and analyzing data, and the second is the increasing online activity of consumers, driven by higher access to high-speed Internet as well as

[14] Anuradha J.,2015,*"A Brief Introduction on Big Data 5Vs Characteristics and Hadoop Technology"*

more online and connected goods and services, including those provided by IoT devices. It is not easy to identify a threshold above which one can speak of Big Data. For a while, the threshold of more than 50 Terabytes or volumes of data growing more than 50 percent annually was considered, but given the large exponential growth, it is not certain that these parameters will remain that way for long.

- Velocity

Velocity refers to the time taken by technological tools to process data and the speed with which it is generated or obtained; example is the one made earlier of how many things happen in just 60 seconds on the Internet. This characteristic of Big Data has also grown to such an extent that traditional data collection and processing techniques are no longer effective.

In some contexts, the value of data is not perishable over time, but it is equally true that for many business opportunities related to the ability to quickly and timely exploit available data, real-time analytics is now a fundamental prerequisite. This demands expertise, technological infrastructure and sophisticated software solutions.

Analyzing data in real time and making decisions at an ever-increasing rate is a capability that companies must improve if they want to have a competitive advantage over co-competition and ensure the best performance.

- Variety

This feature refers to the wide range of information found in a dataset that is generated from different sources and recorded in different formats. The heterogeneity and little organization that make up a raw dataset on the one hand have potentially great value but on the other hand need valid interpretations and reworking to provide correct and useful insights to analysts.

Variety thus represents the need to analyze data from different sources and formats.

- Veracity

The fourth V stands for Veracity and indicates the degree of reliability and thus trustworthiness of the data collected or purchased. Particular attention should be paid to this because of the constant changes to which sources, technologies and systems are subjected over the years that can alter the way data is gathered. Insiders are used to say "Bad data is worse than no data" to indicate that not all data one has has absolute validity, and sometimes analysis of bad information can lead to misleading conclusions that do not fit the purposes initially established. Therefore, the basic pillars of information such as quality and integrity are essential to produce useful and truthful analyses.

- Value

The previous four characteristics serve as the basis for the final "V": data when processed and analyzed represent an invaluable source of value. Therefore, in order to define a set of information as big data, it is not only necessary to have a valid and

selected dataset but also to add tools for targeted and, above all, productive analysis. In fact, without Big Data Analytics, data would not take on the value it has today but would represent only a sterile set of information that cannot be controlled by human capabilities alone.

2.3 BENEFITS ACHIEVABLE FROM THE USE OF BIG DATA

Already in 2006, British mathematician and entrepreneur Clive Humby defined data as the new oil of the 21st century: "Data is the new oil. It's valuable, but if unrefined it cannot really be used. It has to be changed into gas, plastic, chemicals, etc. to create a valuable entity that drives profitable activity; so data must be broken down, analyzed for it to have value."

Companies are increasingly looking for professionals who can analyze data, and this affects not only large companies but also SMEs. A McKinsey article "Catch them if you can: How leaders in data and analytics have pulled ahead" reports how in 2019 46 percent of "top" companies in terms of results had placed a data leader figure on the C-suite team, that is, among the top-level executives in the organization[15].

Interestingly, especially in the digital landscape, the value that Data can generate is so high that companies are sometimes willing to provide them with "free" services

[15] Gottlieb J., Weinberg A., 2019, “Catch them if you can: How leaders in data and analytics have pulled ahead”, McKinsey Global Institute

in exchange for collecting and using consumer data. Renowned is the phrase, "If you are not paying for it, you're not the customer; you're the product being sold." This "new gold" in fact can be exploited for a myriad of reasons that can bring great opportunities to private companies but also to national economies. For example, it is possible to increase a business's profitability by increasing productivity, efficiency and also improving the quality of output[16]. Thanks to data, it is certainly easier to make predictions and consequently make the best decisions in advance. One is able to study people's behaviors and needs by going to analyze their decision-making processes and create models to understand what is the best way to act. Easier and faster access to data also allows for greater transparency as anyone can have access to more information, and data sharing between different organizational units of a company or institution is also facilitated. Services and products are increasingly tailored to customer needs... In summary, data help leaders make smarter decisions about the direction to take and pursue and investing in data leads to gaining competitive advantage in the long run.

2.4 ABUSE OF DATA: CAMBRIDGE ANALYTICA

While it is possible to describe data and their analytics as the new gold because of the many possibilities offered by their analysis, all that glitters is not gold.

[16] Assur N., Rowshankish K., 2022, *"The data-driven enterprise of 2025"*

What is most worrying is the lack of certain principles aimed at preventing the misuse of information and giving some protection to data subjects. Throughout the day, every individual leaves a lot of information behind, and it is not always clear when our data is being collected and stored. Every time, for example, a person makes use of a search engine, he or she leaves a series of digital traces that the owners and operators of the browser collect, store and analyze. The latter will have information about the topics users find most interesting, the sites they use most, when and how they use them, and can process it to offer personalized services and suggestions, making content more appealing to users and, as a result, increasing their revenues both from advertising and from more frequent use of their service. The processing of this data, while very useful for both companies and consumers, is a source of concern because there is the possibility of tracing it back to individuals and violating their privacy and rights. At this point a trade-off arises for users: on the one hand they will receive personalized services tailored to their interests, and on the other they will have to give up much of their privacy. The problem is that the ways that companies use to record such information are often unclear, and people are rarely aware of the sensitive data they are disseminating by operating on a daily basis.

Data entered by users, whether consciously or not, can be used by companies in any way as long as it falls within the range of actions listed once users accept the information. Authorities must control that companies do not use data for improper

and previously unspecified purposes, and at the same time companies must know how to protect their users' information so that it does not fall into the wrong and untrustworthy hands. Data protection regulations and privacy guarantors are not always successful in preventing inappropriate uses, and that is also why continuous updates are needed to make these tools increasingly effective and secure.

One of the most resounding scandals involving the misuse of user data is that of the British consulting firm Cambridge Analytica. In early 2018, it was discovered that Cambridge Analytica had collected without consent the personal data of 87 million accounts on the social network Facebook, a company it worked with, and used them for political propaganda purposes[17]. With access to the PII (Personally Identifiable Information) of these users, it had developed a micro-targeting strategy whereby each individual consumer or voter received personalized messages or offers that could influence behavior in purchasing decisions or even political choices at the voting level.

The case exploded after Cambridge Analytica employee Christopher Wylie declared, "We leveraged Facebook to collect the profiles of millions of people and built models to exploit what we knew about them and target their inner demons. It was on this basis that the whole company was built." Among other things, the

[17] The New York Times, 2018, *"Cambridge Analytica and Facebook: The Scandal and the Fallout So Far"*

former employee claimed that Facebook had known about this violation for as long as two years, which led to Facebook CEO Mark Zuckerberg having to testify in front of the U.S. Congress.

Various political organizations have used this abuse of data to try to sway public opinion; Cambridge Analytica was paid to influence the election campaigns of U.S. politicians Donald Trump and Ted Cruz, The 2016 Brexit case, and the 2018 Mexican elections. This journalistic investigation, carried primarily by The New York Times and The Guardian, has been described as a watershed moment in public understanding of the value of personal data. The investigation strongly challenged privacy laws in the United States but also in the European Union and highlighted how they were seriously flawed. As a result of the incident, there has been a growing awareness among citizens that their personal data if it falls into the wrong hands or is used for illicit and not previously agreed purposes can create serious consequences. Fortunately, also in the same year, the new European Data Protection Regulation 2016/679/EU, commonly known as GDPR (General Data Protection Regulation), became fully operational, which updated previous regulations and imposed an internationally recognized standard as well. The GDPR has certainly placed attention on the accountability of the data controller, and if these new rules had been applied in the area of personal data treatment previously, more security would have been ensured for the benefit of Facebook's registered users.

It has been a long road and there is still a long way to go to improve the use of personal data, but every step is important in order to be able to protect citizens and at the same time allow companies and institutions to take advantage of the great potential that data can offer.

In the next chapters we will try to understand what the evolution of data protection regulations has been and how far we have come at this time; the focus in particular will be on what the European Union has been able to achieve to protect its citizens and businesses.

Chapter 3

EVOLUTION OF DATA PROTECTION IN EUROPE

3.1 THE BIRTH OF THE CONCEPT OF PRIVACY

Since ancient times, man has lived with two conflicting feelings.

On the one hand, human beings are characterized by an innate sense of associationism, almost a survival instinct that has driven them to create communities where they can relate, establish ties, make new acquaintances and discoveries. It has always had the ambition to want to be known by its peers and at the same time to be remembered, leaving an imprint in history.

On the other hand, the human being has felt the need to carve out spaces for himself in order to protect his own private sphere, his emotional relationships with family and friends, and where he can act without the stares and judgments of others. He wanted to isolate his own private dimensional sphere represented by the 4 domestic walls[18].

Already in ancient Greece, with the birth of the first societies, the polis, it is possible to begin to find the distinction between a private and a public sphere of life. However, this separation was not an absolute right but rather a right functional to

[18] Yadufashije C., 2017, *"The reality of human evolution. Human being and evolution"*

the development of the personality of the male citizen so that he would be more ready to participate in public life[19]. With the rise of the bourgeoisie there began to be a need for one's social class to be distinct from others and to have its own identity. The bourgeoisie want to fully enjoy their own intimacy and therefore seek isolation from other social classes.

The modern concept of the "right to privacy" was born in Boston on December 15, 1890 thanks to two young lawyers Samuel D. Warren and Louis D. Brandeis. At that time in America, the print media was evolving greatly with the shift to photojournalism and the publication of mundane events and gossip. Warren himself was constantly targeted by the Boston tabloid newspapers because of his wife's many overt infidelities and eventually decided to write with his colleague Brandeis an expository article in the Harvard Law Review, which is still one of the leading law journals in the United States today.

In this essay, "The Right to Privacy, " the interrelationships between confidentiality to be recognized to an individual, the right of the press to inform, and at the same time the right of citizens to be informed were analyzed in depth.

The ability of journalism during that time to disseminate news widely and quickly meant that even purely mundane facts were delicacies for the insatiable curiosity of

[19] Ostenfeld E, 2016, "Human Wisdom. Studies in Ancient Greek Philosophy"

the nineteenth-century Bostonian bourgeoisie. In doing so, facts not only concerning citizens who held specific public offices but also private affairs without any kind of relevance became public knowledge.

The two lawyers found themselves, therefore, pondering which information concerning an individual's personal life should be in the public domain and which, on the other hand, deserved protection from the intrusiveness of others. The publication of the two lawyers was the first legal paper ever to recognize the existence of an autonomous right to privacy, better defined as "the right to be let alone."

Warren and Brandeis reconnected with the right to property (very much in vogue and dear to the liberal model of the time) but in this case they were going to include non-material aspects such as feelings, thoughts and emotions, which until then had not yet received any protection. Warren and Brandeis invite American judges to start guaranteeing the right to privacy in their rulings and make it a common law right.

The published essay specifies that "The right to privacy does not prohibit any publication of matter which is of public or general interest," and at the same time that "The right to privacy ceases upon the publication of the facts by the individual, or with his consent."

Although the time was not yet mature and the voice of the two lawyers remained largely unheard it must be acknowledged that the great insight of this article was to

shift the attention of the American legal landscape to the true dimension of the right to privacy, understood no longer as an extension of the right to property, but having a strictly individual dimension linked to the personality of the individual.

3.2 EUROPE AS MAIN PROMOTER OF THE RIGHT TO PRIVACY: ART. 8 ECHR

Europe is the place par excellence where the right to privacy has been and is being promoted.

The tragic experiences of totalitarian regimes in the first half of the twentieth century consolidated in the European mentality the value that must be placed on a protection of people's privacy. During Nazism and Fascism, governments aimed at the alienation of the individual, depriving him of freedom and making him embrace the ideology of the party, taking away his faculty of choice, but comforting him with propaganda in a reassuring dictatorship in which people had only to limit themselves to following the rules without thinking. Citizens were thus deprived of their personal sphere, and the Nazi metaphor of the "glass man" explains this concept very well: the state had the claim to be able to demand and obtain any information from its citizens who would be classified as suspicious and bad if they

wanted to maintain spaces of intimacy, in other words, if they had something to hide from the regime[20].

If someone is deprived of his privacy, his ability to act and think is also restricted, and the loss of freedom expands to every other aspect of his life, making him more of an automaton than a person. Privacy, conversely, thus becomes a prerequisite of democracy.

After living through this dark period, the priority was to protect the individual and his freedoms, and to prevent similar horrors and disasters from happening again in the future. Initially, the impetus for the promotion of the right to privacy was infused by the very important work of the Council of Europe, a regional organization with a universal vocation, born from the ashes of World War II.

The Council of Europe was founded in 1949 by the Treaty of London, is headquartered in Strasbourg, and today has 46 members; after the attack on Ukraine, the Russian Federation was suspended and on March 15, 2022, permanently ended its relationship with the organization. Given the great confusion that often exists about these bodies, it is important to specify that the Council of Europe is outside the European Union and should not be confused with organs of the latter, such as the Council of the European Union or the European Council.

[20] Ziegler H., 2014, *"Nazi Germany's New Aristocracy"*

Within a year of its founding, the Council of Europe had already drafted a document to promote democracy and safeguard human rights. This took the name European Convention for the Protection of Human Rights and Fundamental Freedoms, or more simply ECHR, and on September 3, 1953 it actually came into force, becoming the most important legal instrument on rights at the European level.

Of all the articles in the convention the one that is most internationally relevant to "privacy" is Article 8, right to respect for private and family life:

1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

The two clauses are very simple and clear to understand however what is quite surprising is that the word "privacy" is never used in the article, although this article is recognized as one of the most important ones dealing with this topic. In the original draft the term privacy was used but after several revisions and before final publication, this term was changed and now "private life" appears in the final version. This is due to the strong French influence that uses the term "vie privée" in its language.

The two terms may seem similar but there are substantial differences, in fact the right to privacy is defined as "the right to be let alone" and this thus includes both respect for "private life" but also the right to personal autonomy and self-determination. The concept of "privacy" is therefore a broader and more nuanced concept than that of "private life."

In the first decades after the adoption of the ECHR, the European Court of Human Rights (also known as the Strasbourg Court) systematically avoided using the word "privacy" to refer to the rights protected by Article 8. This Court is the international court responsible for safeguarding and ensuring the application of the ECHR and is consequently the ultimate interpreter of this article.

3.3 THE TERM "PRIVACY," ELECTRONIC DATABASE RESOLUTIONS, AND "DATA PROTECTION"

The situation begins to change in 1967 when the Council of Europe opens a debate about the impact of scientific and technological development in the protection of human rights and questions whether Article 8 adequately protects the right to "privacy" (this exact term is used) against violations that can be committed through the use of new scientific and technological methods. A committee of human rights experts is then created to highlight how new technologies, especially computers, can be a great risk to citizens' privacy. The main problem of Article 8, which from

now on will be regarded as a protection precisely to the right to "privacy," is that the provision can be applied only to interference by public authorities and not to interference by private parties, and consequently the protection needs to be updated and expanded.

On September 26, 1973, Resolution (73) 22 "on the protection of the privacy of individuals vis-a-vis electronic data banks in the private sector" was adopted. The resolution, which takes the form of a recommendation to member states (and is therefore not legally binding), contains a list of principles that apply to personal data recorded in electronic databases in the private sector. The most important principles concern: the quality of the information, the purposes of the information, the means by which the information is obtained, the retention period of the data, the data subject's right to information, deletion and rectification of information, measures to prevent misuse, and access to information.

Since Resolution (73) 22 deals exclusively with databases in the private sector, the Council of Europe on September 20, 1974, adopted a second instrument which, on the contrary, applies only to the public sector: Resolution (74) 29, "on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector." This act, again, takes the form of a Recommendation to member state governments and contains a list of principles.

These resolutions, although not binding, are important because they are the first example in history where the right to privacy also begins to cover new scientific and technological tools. People are beginning to realize how new technologies can have an impact on the lives of states and citizens and therefore, how important it is that these aspects should also be controlled[21].

As early as late 1974, experts of the Council of Europe believed that the body of law created in the Old Continent for the protection of individuals against computerized collections should be referred to by a specific name: "data protection." This notion can be defined as the set of rules and legal instruments designed to protect the rights, freedoms, and interests of individuals whose personal data are recorded, processed, and disseminated by computer from unlawful intrusion, and to protect recorded information against unauthorized, accidental, or intentional alteration, loss, destruction, or disclosure. Accordingly, this body of law is brought under the umbrella of "privacy."

3.4 CONVENTION 108, 1981

After adopting Resolutions (73) 22 and (74) 29, the Council of Europe decides to continue its work, monitoring their impact and, in general, the progress made by

[21] Mun S. Ho, Fisher-Vanden K., 2010, *"Technology, development, and the environment"*

national legislation in this area. The study highlights the existence of disparities between nations, which are deemed to be a problem warranting further action. Indeed, it is important to remember that the resolutions were non-binding and therefore each state could move independently.

In 1976, a Committee of Experts on Data Protection was created, whose goal was to finalize a Convention (this time therefore mandatory for signatory states) for the protection of privacy with respect to the processing of personal data by 1980 The Committee, from the very beginning, comes into contact with the Organization for Economic Cooperation and Development (OECD), with which it starts a relationship characterized by cooperation and mutual aid: the common idea, in fact, is that the future Council of Europe Convention should respect the principle of non-restriction of transborder flows of personal data, a principle very dear to the OECD. Taking up the proposal of one of the experts and after a long series of debates, it was decided to draft a Convention that could be ratified not only by European states, but also by non-European countries. Although elaborated in a regional context therefore, it is an instrument with a universal vocation, and precisely for this reason it does not take the name European Convention, but exclusively Convention[22]. The final version of the "Convention for the Protection of Individuals with regard to

[22] Council of Europe, 1981, *"Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data"*

Automatic Processing of Personal Data" is published in April 1980 and opened for signature on January 28, 1981, in Strasbourg.

3.4.1 The content of Convention 108

To understand what the convention is about, it is enough to refer to the first provision.

Article 1: Object and purpose.

The purpose of this Convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection").

From this article, three fundamental innovations emerge that make Convention 108 a true milestone in the field of personal data processing disciplines:

- The term "data protection" is included for the first time in a legally binding instrument of international law.
- It formally links data protection to the protection, in general, of fundamental rights and freedoms.
- A special link is established between data protection and the right to "privacy," and by this notion is undoubtedly meant the right enshrined in Article 8 of the ECHR. Thus, for the purposes of the Convention, there is something called "data protection" that is regulated to preserve something called "privacy."

3.4.2 The objectives of Convention 108

The OECD Guidelines have two objectives that may seem at first glance to be in conflict one with the other: privacy and the free flow of personal data across borders. Instead, Convention 108 has, at least formally, only one purpose that is to ensure data protection.

However, reading the text of the Convention, one realizes that from a substantive point of view things are different since it also deals with ensuring the free flow of data. Chapter III, in fact, is devoted to "Transborder data flows," and states that a Party may not, for the sole purpose of protecting privacy: "prohibit or subject to special authorization transborder flows of personal data going to the territory of another Party" (Article 12 paragraph 2). The implicit assumption, of course, is that the Contracting Parties provide an equal level of protection.

The free flow of personal data relates, even if rather indeterminately, to both the notion of free markets and freedom of expression. Indeed, according to Article 10 paragraph 1 of the ECHR, freedom of expression includes "the freedom to receive or impart information or ideas without interference by public authority and without boundary limits." The very preamble to Convention 108 defines the free flow of information among peoples as a fundamental value.

So, in conclusion, although formally the Convention does not aim to ensure the free flow of data, it does address this issue in several articles.

Regarding to the field of application of the Convention, however, it is defined in Article 3 paragraph 1 of the Convention that it extends to "automated personal data files and automatic processing of personal data," both in the public and private sectors.

Although Convention 108 covers only and exclusively automated processing, it is nevertheless a truly broad area of application, extending to every sector of society such as labor, banking, insurance, commerce, schools, health, police, justice, and public administration. Under paragraph 2 of Article 3, however, the contracting states enjoy considerable discretion in narrowing or broadening this scope, both with regard to the categories of collections and the categories of stakeholders.

Also worth noting is that for the purposes of the applicability of these regulations, the form under which the data are processed or used is not specified: as demonstrated by the practice and jurisprudence of the European Court of Human Rights, they can be contained in both written and oral communications, in images, video footage, GPS positioning systems, detections from closed-circuit television systems, cellular samples of human tissue, and in other possible configurations.

3.4.3 The principles of Convention 108

Important data protection principles can be grasped from the text of the Convention, which will prove fundamental to the evolution of the law itself and will also be adopted by subsequent major acts (e.g., the European Union acts) on the subject.

First of all, the Convention in Article 2 gives the definitions of "personal data" and "automatic processing," defining the former as "any information relating to an identified or identifiable individual ("data subject")" and the latter as an activity that "includes the following operations if carried out in whole or in part by automated means: storage of data, carrying out of logical and/or arithmetical operations on those data, their alteration, erasure, retrieval or dissemination."

Further important provisions regarding data are considered in the following articles. Article 5 entitled "Quality of data" describes the characteristics and modalities for personal data to be deemed of adequate quality. They must be:

(a) Obtained and processed fairly and lawfully;

(b) Stored for specified and legitimate purposes and not used in a way incompatible with those purposes;

(c) Adequate, relevant and not excessive in relation to the purposes for which they are stored;

(d) Accurate and, where necessary, kept up to date;

(e) Preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.

Another fundamental principle is the one stipulated in Article 6 where a special category of so-called "sensitive" data is introduced in order to provide an adequate response to the growing fears of a public opinion increasingly wary of indiscriminate filing of people's most intimate aspects or of discriminatory attitudes

based on such data. In fact, sensitive data are composed of that type of information characterizing a person and capable of detecting racial origin, political opinions, religious beliefs, health status and sexual orientation as well as those related to an individual's criminal convictions. Such data, it is prescribed in Article 6, may not be processed by automated techniques unless appropriate safeguards are provided. It is necessary to specify that the processing and circulation of this type of data is generally prohibited not only on the basis of the "intimacy" of the information, but especially because, more than other types of data, these can be a source of discrimination and as such, an obstacle to the development of an individual's personality especially within society.

Proceeding to the analysis of the Convention, Articles 7 and 8 respectively regulate "Data security," so that unauthorized dissemination does not take place, and "Additional safeguards for the data subject" to whom must be granted certain faculties inherent in the knowledge and management of his or her data such as: the purposes for which the data are kept, the identity and residence/administrative headquarters of the person in charge of the record and having the possibility of obtaining the rectification or deletion of such data if processed in violation of the principles set out in Articles 5 and 6.

The principles described so far are provided to be generally applicable, but not to be regarded as absolute. In fact, peremptory conditions are provided in Article 9 for which a state may derogate from the principles expressed in the preceding articles.

Still considering "democracy" and "necessity" of the measure as parameters of legitimacy of state action and protection of fundamental rights, the derogation may operate for:

(a) Protecting state security, public safety, the monetary interests of the state or the suppression of criminal offenses;

(b) Protecting the data subject or the rights and freedoms of others.

The Strasbourg Convention has been and continues to be a document of great legal importance in the field of personal data protection. It represents the authentic final piece in the long journey that led to the definitive understanding and recognition of the right to the protection of personal data as a true fundamental right protecting the freedom of individuals, separated now from the "mother" concept of privacy[23]. Moreover, it represents an undeniable turning point since, by standing as supranational legislation, it changes "the rules of the game" by establishing once and for all the principles that can no longer be disregarded by state legislatures and by indicating the first step on the road ahead for future legislating of personal data protection.

[23] O'Connell R., 2010, *"Social and Economic Rights in the Strasbourg Convention"*

3.5 STEPS TOWARD THE CREATION OF EUROPEAN DATA PROTECTION LEGISLATION

Convention 108/1981 was created with the aim of creating a uniform level of personal data protection throughout Europe. For this reason, after its adoption, the Commission repeatedly called on the individual member states of the European Economic Community (EEC) to ratify the Convention, in order to have an equal level of protection all over the territory.

In the first half of the 1980s, the EEC continued to promote studies on the subject, and in particular, in April 1984, the Council undertook to co-fund research on the privacy and security of personal data, aimed at examining the legislation in force or under preparation in the member states, as well as considering possibilities for harmonizing disciplines[24]. However, the diversity of approaches taken by member states put European integration at risk, and the Commission affirms the need to introduce EU rules on the protection of individuals in relation to the processing of personal data. The main differences between national legislations that Convention 108 failed to reduce in a significant way relate mainly to two points:

- The field of application: some disciplines also apply to legal persons, others do not; some disciplines also apply to non-automated (i.e., manual) processing, others do not.

[24] Giakoumopoulos C, O'Flaherty M., Buttarelli G., 2018*, "Handbook on European data protection law"*

- The preconditions of processing, such as information requirements at the time of collection and conditions for processing sensitive data were legislated differently from state to state.

The Commission to justify its action then also refers to the many requests, coming mainly from the European Parliament, to take action in the field in order to approximate national regulations.

In those years, Europe witnessed a major initiative, which is still considered one of the key steps in European integration: the Schengen Agreement. The Schengen Agreement is an international treaty on the gradual abolition of common border controls among the five signatory countries: Belgium, France, Germany, Luxembourg, and the Netherlands (all also member states of the EEC). The Agreement is signed on June 14, 1985, but the actual abolition of border controls is conditional on the adoption of additional measures, detailed in a second instrument: the Convention Implementing the Schengen Agreement (or, more simply, the Schengen Convention), signed by the same states in 1990. The agreement will become effective in 1995.

For the purposes of this thesis, it should be mentioned that the 1990 Convention establishes the Schengen Information System, or SIS, a common archive for all the states in the Schengen area consisting of a national section at each adhering country and a technical support unit in Strasbourg in which information on wanted persons

or persons placed under surveillance, and information on wanted objects (such as vehicles or identity documents), are specifically contained[25]. The Convention devotes an entire Chapter to "Protection of Personal Data and Data Security in the Framework of the Schengen Information System," a Chapter in which the Article 117 paragraph 1, stipulates the obligation of the Contracting Parties to adopt internal provisions guaranteeing "a level of protection of personal data at least equal to that resulting from the principles of the Council of Europe Convention of January 28, 1981." In addition, Article 114 paragraph 1 obliges each adhering country to designate a supervisory authority responsible, in accordance with national law, for exercising independent supervision over the national section of the SIS and for "verifying that the processing and use of data entered therein does not infringe the rights of the data subject." Also worth mentioning is Article 112, which establishes the principle that personal data entered into the SIS "shall be kept only for the period necessary for the purposes for which they were provided." Finally, Article 115 establishes a joint supervisory authority, composed of two representatives from each national supervisory authority.

Another fundamental step, considered to this day as a milestone for the process of European integration, is the Maastricht Treaty signed on February 7, 1992, which

[25]Inshakova A., 2019. *"The Schengen Information System: legal support for the automated cross-border business management"*

transforms the EEC into the European Union and defines its so-called three pillars: the European Communities, the Common Foreign and Security Policy and cooperation in justice and home affairs. We are moving ever closer to the Single Market that was a goal as early as 1957 when the Treaty of Rome was signed and the European Economic Community was first established. The aim is to achieve full implementation of the four symbolic freedoms of Community integration: the free movement of goods, persons, capital and the freedom to provide services. To do this, it is essential to overcome even the intangible borders constituted by different national data protection laws. This requires adequate and up-to-date legislation on personal data (and fundamental rights in general) emanating from the EU, so as to make the functioning of the Single Market efficient and, at the same time to redesign the jurisdiction for all those disputes concerning fundamental human rights violated within the dense networks of the EU system. In addition, the differences between national legislations that Convention 108 had failed to reduce and had been carried on for several years, were also to be settled.

This was accomplished through the adoption of two important acts by the European Union: first with Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data; later with the promulgation of the Charter of Fundamental Rights of the European Union proclaimed in Nice and included in the Lisbon Treaty that came into force in 2009.

3.6 DIRECTIVE 95/46/EC

On October 24, 1995, the European Parliament and Council approved Directive 95/46/EC "on the protection of individuals with regard to the processing of personal data and on the free movement of such data."

For a long time, European Directive 95/46/EC has been the reference text, at the European level, on the subject of personal data protection. It must be said from the beginning that the Directive refers as much to Article 8 of the ECHR as to Convention No. 108/1981, but it undoubtedly specifies and amplifies its content and scope, sometimes overturning guidelines established by previous legislation on the subject. At that time, the European Union was still divided into the traditional three-pillar structure, of which: the first pillar addressed the European Communities (EEC), the European Common Market, and Economic and Monetary Union; the second dealt with the Common Foreign and Security Policy (CFSP), that is, the construction of a single outward-looking policy; and the third, Judicial and Police Cooperation in Criminal Matters, was aimed at the construction of a European area of freedom, security and justice, in which there was cooperation against crime at the supranational level. So, the framework of the '95 directive was born within the framework of the European Community and therefore intended to operate under the first pillar. For the first time, on European territory, in order to increase the effectiveness of the four freedoms, the single market and the free development of the personality of the individual, the EU was responding with a common legislation

such as to guarantee specific protection to the data of individuals who, since the breaking down of borders, were yes freer in movement, but at the same time more vulnerable from "borderless" attacks.

Perhaps one would have expected from the European legislature a different form of the act through which to implement the common framework on personal data protection, more likely a regulation (the instrument that will in fact be chosen for the 2016 framework). Given the characteristics of the regulation such as its broad application, its mandatory nature in all its elements, and its direct applicability, it would undoubtedly have been the most appropriate means in order to avoid disputes, explanatory gaps, or different interpretations between one country and another. The European legislator, however, opted for the adoption of a harmonization directive with the aim of establishing the general and founding principles of the subject matter and a set of rules, not having an immediately binding character, but which would have obliged the Member States to adapt their national legislations to it within the time limit set by the directive itself[26]. In any case, the Directive has proved over time to be an agile and useful tool by fostering, on the one hand, a process of homogenization of the levels of protection of rights, regardless of the state system of reference, and, on the other, by enriching the content of the rights recognized by individual Constitutions.

[26] Wong R., 2012, *"The Data Protection Directive 95/46/EC: Idealisms and Realisms"*

3.6.1 The objectives of the Directive

To understand what the objectives of this Directive are, it is enough to go to Article 1 of Chapter I. This consists of two paragraphs that identify the two main objectives that the Directive aims to achieve.

Paragraph 1 identifies as its first objective the protection of the fundamental rights and freedoms of natural persons, and particularly the right to "privacy," with regard to the processing of personal data.

The 1995 Directive undoubtedly takes up the approach of Convention 108 of 1981, whereby the protection of personal data is functional to the protection, in general, of fundamental rights and freedoms, but particularly of the right to privacy. Even in the Preamble of the Directive, the right to "privacy" is defined as "also recognized by Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms"; but in fact, it is worth repeating, Article 8 of the ECHR uses the expression "private life" and not "privacy." Therefore, according to the European institutions, the two notions are perfectly synonymous.

Paragraph 2 of Article 1, on the other hand, identifies the "free movement of personal data between member states" as the second objective of the Directive.

With regard to the second objective, however, it is important to note that according to the Preamble of the Directive, "the establishment and functioning of the internal market, in which, in accordance with Article 7 of the Treaty, the free movement of goods, persons, services and capital is ensured, require [...] that personal data should

be able to move freely from one Member State to another." The interconnection between the free movement of personal data and the four fundamental freedoms of the internal market thus seems clear. On the other hand, it is not clear whether, more precisely, the free flow of data is functional to the free movement of goods, persons, services, or capital. In the opinion of many, the first option is preferable. Indeed, the notion of "goods" can be defined as the "products that can be valued in money" and "the subject of commercial transaction." However, nowhere is it specified that we are talking about tangible goods, and even the fact that it must constitute an object of commercial transaction should not be read too strictly.

Already in the 1980 OECD Guidelines there was an intent to reconcile these two opposing requirements, which were described by the terms "Protection of Privacy" and "Transborder Flows of Personal Data." From there on, all international instruments on the subject, though to varying degrees, attempt to balance the two objectives but Directive 95/46/EC, by mentioning them from its very first article, and devoting a paragraph of its own to each, certainly intends to reinforce the meaning of both, as well as to make clear their nature as conflicting values.

3.6.2 The content of the Directive

The second article, it is instead devoted to "Definitions." In fact, having clear and

well-defined definitions from the outset helps to better understand the contents of the Directive's articles and avoid misunderstandings.

According to Article 2, letter a, it is possible to speak of "personal data" in the presence of "any information relating to an identified or identifiable natural person ('data subject')." Subparagraph (a) goes on to specify that "an identifiable person is one who can be identified , directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity." Thus, the core of the definition remains unchanged from the first instruments of international law on the subject (OECD Guidelines; Resolutions 1973-1974 and Convention 108 of the Council of Europe); on the other hand, this notion is considerably clarified by adding much more detail.

Definitions of other terms such as "'processing of personal data,'" "personal data filing system," "controller," "processor," "third party," "recipient," and "the data subject's consent" are also given.

Continuing in the next article, it is specified when this set of laws is to be used, i. e., the field of application of Directive 95/46/EC.

According to Article 3 paragraph 1, "This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system."

This field of application, therefore, is broader than that of Convention 108, which on the contrary covers only the automated processing of data.

There are, however, two important exclusions. According to Article 3 paragraph 2, in fact, "This Directive shall not apply to the processing of personal data:

- in the course of an activity which falls outside the scope of Community law [...] and in any case to processing operations concerning public security, defense , State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law;
- by a natural person in the course of a purely personal or household activity."

3.6.3 The principles, consent and sensitive data of the Directive

Going to analyze Article 6, which sets out the "Principles relating to data quality," it is easy to see that these principles have remarkable similarities with Convention 108. The principles are the same 5 as in the previous Convention and indicate that data must be:

- processed fairly and lawfully:
- collected for specified , explicit and legitimate purposes and not further processed in a way incompatible with those purposes;
- adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;

- accurate and, where necessary, kept up to date;

- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed.

However, more information is also specified at each point (not shown here) to make these principles even clearer for individual member states; Convention 108, on the other hand, remained much simpler without going into too much detail.

There is one aspect that Directive 95/46/EC puts much more emphasis on than Convention 108: the issue of consent. While consent was previously given a definitely marginal role, now the six conditions that make data processing lawful are found in Article 7. The first of the 6 conditions, and also the most important, is the circumstance where "the data subject has unambiguously given his or her consent." Some other cases where data processing is lawful are, for example, when it is necessary to protect the vital interests of the data subject, to fulfill a legal obligation, to perform a public interest task, etc...

Article 8 of the European Directive deals with another very important aspect: special rules for "processing concerning special categories of data," (most often recognized as the "sensitive data"). Paragraph 1 prohibits, in principle, "the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of data concerning health or sex life"; the paragraphs immediately following, however,

establish exceptions. In contrast, the rules concerning "processing of data relating to offenses, criminal convictions or security measures" are different: according to paragraph 5, in fact, they must be carried out under the control of the public authority or be accompanied by "specific safeguards." In making ad hoc provisions for certain categories of data, the Directive is undoubtedly influenced by Convention 108, specifically Article 6, which is devoted to "special categories of data." There are divergences, however, between the two articles, both in terms of the categories listed and the discipline provided: indeed, Article 6 of the Convention merely requires "suitable safeguards" for all data in the catalog.

For the sake of completeness, other important provisions addressed by Directive 95/46/EC are also quickly reviewed:

- Right of access to data by the data subject to obtain erasure or rectification of data;
- Right to object to certain processing operations;
- Obligations regarding confidentiality and security of processing;
- Exceptions and restrictions to limit the scope of obligations and rights;
- Transfer of personal data to third countries (is authorized only if the receiver has an adequate level of protection);
- Development of data protection codes of conduct;

- Obligation to establish at the national level one or more public authorities responsible for supervising the application of the provisions implementing the Directive.

3.7 IMPACT OF THE DIRECTIVE ON NATIONAL DISCIPLINES: FOCUS ON ITALY

As already specified, the directives are not immediately applicable; on the contrary, they require transposition by the member states, transposition which must take place within a certain period of time. Directive 95/46/EC, in particular, obliges member states to adapt their national legislation within 3 years.

At the time of the adoption of this legal instrument, only two member states had not yet passed a personal data protection law: specifically, Greece and Italy. But a good number of other states, while having legislation on the subject, still needed to amend it in order to bring it in line with the provisions of the 1995 Directive. However, the work of transposition turns out to be much more laborious and, above all, significantly slower than the Commission expected[27]. It got to the point that the latter, in 1999, initiated a series of infringement proceedings against a number of countries guilty of not yet having adopted implementing provisions: in this case, France, Germany, Ireland, Luxembourg and the Netherlands.

[27] Korff D., 2002, *"EC Study on Implementation of Data Protection Directive 95/46/EC"*

Moving into detail, the first state to transpose Directive 95/46/EC is Italy. After signing Convention 108 in 1983, Italy immediately prepared a legislative proposal on data protection, but over the years failed to pass it into law. Under new impetus from the Directive, Law No. 675 on the "Protection of Persons and Other Subjects with Respect to the Processing of Personal Data" (in Italian “Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali”) was finally passed on December 31, 1996, allowing Italy to ratify Convention 108, enter the Schengen Area and, of course, comply with the Directive of the previous year. The 1996 Law introduces into Italian law the "right to privacy" and the "right to personal identity." Its purpose is described by the first paragraph of Article 1, according to which this law guarantees that the processing of personal data is carried out with respect for the rights, fundamental freedoms, and dignity of natural persons, with particular reference to confidentiality and personal identity; it also guarantees the rights of legal persons and any other entity or association. This is, according to Stefano Rodotà (an Italian jurist, politician and academic), an improvement over the formulation contained in Directive 95/46/EC.

Since 1996, therefore, the word "privacy" has also begun to be used in Italy. Actually, this term does not appear in Law No. 675; but when referring to the latter, the doctrine often uses the expression "privacy law."

Thanks to this legislation, the " Data Protection Authority," also known as the Privacy Guarantor, is established. This figure is an independent Italian

administrative authority whose objective is to ensure the protection of fundamental rights and freedoms and respect for dignity in the processing of personal data. it consists of four members (one of whom is the president), elected by the two branches of the Parliament of the Italian Republic whose term of office is set at seven years, non-renewable. In order to carry out its objectives and protect the interests of citizens, the guarantor enjoys a number of powers including: adopting guidelines and codes of conduct; organizing on-site inspections and requesting access to documents and databases; imposing administrative sanctions; ordering the rectification or deletion of personal data, imposing a temporary or permanent restriction on their processing, and even banning them. Just to give an idea of the large amount of work this authority has to do: according to Openpolis in 2019, the Privacy Guarantor received 9,689 reports and complaints[28].

3.8 OTHER ACTS BEFORE THE GENERAL DATA PROTECTION REGULATION OF 2016

- Regulation (EC) No. 45/2001

Since the effects of Directive 95/46/EC were addressed only to states, there was a need for a regulation so as to extend the protection of personal data also to treatment

[28] Openpolis, 2020, *"Cosa fa il garante per la protezione dei dati personali (garante della privacy)"*

carried out by EU bodies and institutions. The submission of the proposal was made by the European Commission in 1999, and after a rather short legislative process, Regulation (EC) No. 45/2001, "on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data," was adopted on December 18, 2000.

Article 1 provides a better understanding of the meaning of the expression "free movement," which indicates the flow of data both between Community institutions and bodies and between them and recipients subject to the implementing provisions of the 1995 Directive. In addition, still in the first article, there is a concretization of the idea of having also in the European Union an independent supervisory authority whose task is to monitor the application of the provisions of the Regulation itself to all processing of personal data carried out by a Community institution or body. This authority is called the "European Data Protection Supervisor" (or EDPS) and the activities that this can perform can be divided into three main roles: supervision, consultation and cooperation. Citizens, for example, can appeal to the EDPS to make a complaint if they feel that one of their rights has been infringed upon by non-compliance with the regulation. The EDPS is regulated in detail by Chapter V of the 2001 Regulation.

- Regulation (EC) No. 1049/2001

Regulation (EC) No. 1049/2001 of the European Parliament and of the Council,

deals with public access to European Parliament, Council and Commission documents. The Regulation is based on the idea that "all documents of the institutions should be accessible to the public." But there are also exceptions, the most significant of which (at least for our purposes) is enshrined in Article 4(1)(b), according to which the institutions shall refuse access to a document the disclosure of which would undermine the protection of the "privacy" and integrity of the individual, "in particular in accordance with Community legislation on the protection of personal data."

- **Directive 2002/58/EC**

In 1997, Directive 97/66/EC "concerning the processing of personal data and the protection of privacy in the telecommunications sector" was adopted. However, this act will be replaced a few years later by Directive 2002/58/EC, which again deals with the electronic communications sector and whose provisions specify and supplement Directive 95/46/EC by going on to legislate a particular scope.

Directive 2002/58/EC especially regulated "traffic data," which must be erased or anonymized at the end of the call; however, in cases of security, defense and crime prevention these data may be retained for a limited period of time. In addition, in the case of breaches that lead to a personal data breach, providers are obliged to notify the national data protection authority and in some cases, depending on the

type of data compromised, must also notify the data subjects.

- **Directive 2006/24/EC**

On the just mentioned issue of retention of such data comes back Directive 2006/24/EC of the European Parliament and of the Council of March 15, 2006, concerning the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC. According to Article 1 paragraph 1, "The purpose of this Directive is to harmonize the provisions of the Member States concerning the obligations [...] relating to the retention of certain data [...] for the purpose of ensuring their availability for the investigation, detection and prosecution of serious crime." The "categories of data to be retained" are listed in Article 5, while, according to Article 6 the "retention period" must be no less than 6 months and no more than 2 years.

The need for the adoption of more stringent and effective legislation, common at the European level, became more pressing especially following the terrorist attacks in Madrid and London in 2004 and 2005. The terrorist attacks, which were also claimed by the jihadist Al Qaeda network, created a very strong sense of instability and concern within the European Union.

However, this Directive did not have a very long life, in fact the Irish High Court and the Austrian Constitutional Court raised the question of the legitimacy of the

directive to the European Court of Justice, which in a ruling on April 8, 2014 declared the directive invalid, and therefore ineffective since its entry into force. According to the European Court, the directive was disproportionate to its objective, censuring the non-"targeted" nature of the surveillance measure and the possibility of indiscriminate access by authorities to retained data.

- **Charter of Fundamental Rights of the European Union and the Lisbon Treaty of 2007**

The Charter of Fundamental Rights of the European Union, proclaimed in Nice in 2000, represented another small step forward for the right to personal data protection. The Charter was created in response to an increasing demand for legal certainty within the complex economic, commercial and jurisdictional dynamics facing the European Union, especially in the area of human rights[29].

Initially, the possibility was considered for the European Community to accede to the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), which protected human rights and was overseen by the European Court of Human Rights. This option, however, was set aside when the European Court of Justice stated that: "the incorporation of the Community into a separate international institutional system [...] would result in a substantial

[29] Ciuca A., 2012, *"On the Charter of Fundamental Rights of the European Union and the EU Accession to the European Convention on Human Rights"*

modification of the Community's existing human rights protection regime." Given the various difficulties, it was therefore preferred to adopt its own Charter of Fundamental Rights, entrusting the Court of Justice with the power to ensure its proper application.

Originally, no binding legal value is given to this Charter, but the situation finally changes in 2009, when the Lisbon Treaty enters into force. Article 6(1), in fact, provides that "the Union shall recognize the rights, freedoms and principles set out in the Charter of Fundamental Rights of the European Union of December 7, 2000, adopted on December 12, 2007, in Strasbourg, which shall have the same legal value as the Treaties."

The main purpose of the Charter was to make EU citizens more aware of the primary importance and relevance of fundamental rights. As far as the right to personal data protection is concerned, the Nice Charter is fundamental because for the first time, on a text of a "constitutional" nature, having general and supranational value, the right to the protection of personal data was enshrined as an autonomous right distinct from the right to privacy. Two articles of the Nice Charter are of significant importance : Article 7 and, even more so, Article 8.

Article 7: Respect for private and family life

"Everyone has the right to respect for his or her private and family life, home and communications".

Article 8: Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority.

It can be seen that other documents such as the ECHR, Convention No. 108/81, and Directive 95/46/EC are taken very much as models. The real novelty, in the end, lies in the fact that the elements mentioned in the Nice Charter are now to be protected as components of a fundamental right, which deserves protection in its own right; moreover, protection is no longer granted exclusively to data that, in one way or another, can be considered as "relating to private life," but to personal data as such. And from this point of view, the protection offered by the Charter of Fundamental Rights of the European Union goes far beyond that of the ECHR, and even beyond that of the common constitutional traditions of the member states.

All these acts we have analyzed trace the history and evolution of the right to privacy and personal data protection in Europe. The next chapter will look in detail at the most recent Regulation of 2016, which retires Directive 95/46/EC and introduces a new and more robust framework for the protection of personal data.

The "General Data Protection Regulation," or GDPR, seeks to create a bridge between the past, present, and future of the subject under consideration and has important and innovative implications for any organization in the world that deals with EU citizens.

Chapter 4

THE GENERAL DATA PROTECTION REGULATION

4.1 THE ADOPTION OF REGULATION (EU) 2016/679

EU Regulation 2016/679 marks the advent of a new era for the world of privacy.[30] The intent of the legislature was certainly to provide legal stability to the data protection discipline within the EU territory, but also to give European companies greater competitiveness on the international market, since in a becoming digital economy it is crucial to gain the full trust of consumers.

To meet the new challenges thrown up by globalization and pressing technological developments, the European Parliament approved the General Data Protection Regulation (GDPR) in April 2016, which officially enters into force on May 24, 2016. However, its application will formally take effect on May 25, 2018, after a useful two-year timeframe for member states to better organize their national regulatory framework so as to effectively incorporate the Regulation within their own legal system.

Already in the choice of medium the revolutionary intent of this act is recognized: no longer a harmonization Directive that seeks, through the action of the Member

[30] Grest L., Ryz L., 2016, *"A new era in data protection"*

States, to approximate legislation and juridical cultures as much as possible, but a strong legal instrument having a binding character and so, mandatory in all its parts and directly applicable in all EU Member States.

This Regulation after more than two decades of application definitively repeals Directive 95/46/EC.

4.1.1 The objectives of the Regulation

To analyze the Regulation, it is impossible not to start from Article 1: "Subject-matter and objectives."

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

2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

3. The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.

This provision has some similarities but also a major difference from Directive 95/46/EC and all previous EU legal instruments on the subject.

The biggest similarity is that as in the OECD Guidelines, Convention 108, and Directive 95/46/EC, it speaks of a dual objective namely the protection of

individuals with regard to the processing of personal data and the free movement of such data, just as in Article 1 of the GDPR. In addition, the wording of paragraph 3 regarding the free movement also echoes the same structure used in previous acts. The big difference, concerning the first of the two objectives, however, lies in paragraph 2, and consists in the expression "in particular their right to the protection of personal data," which is also used in the Preamble of the Regulation. In all previous documents (Directive 95/46/EC, Directive 97/66/EC, Regulation EC No. 45/2001, and Directive 2002/58/EC) there was always the same formula under which the protection of personal data is functional to the protection of fundamental rights and freedoms, but in particular the right to "privacy." In the 2016 Regulation, the right to privacy no longer appears and the right to personal data protection replaces it completely. There is a great difference between these two terms, and the different approach has very significant repercussions on the institutions governed by Regulation 2016/679.

The right to "personal data protection" does not merely exclude the interference of others and offer "static" protection like the right to "privacy." On the contrary, it takes the form of powers of control and intervention: the protection is "dynamic," following the data as they circulate. Moreover, with this substitution, protection is no longer granted exclusively to data that, in one way or another, can be considered as "relating to private life" (privacy), but to personal data as such. This means the protection of personal data is not partial, but full.

4.1.2 Material scope and territorial scope

Articles 2 and 3 specify what the scope of the Regulation is by distinguishing between material and territorial scope.

Regarding the material scope, it is possible to see that this remains practically unchanged. The 2016 Regulation applies to wholly or partially automated processing of personal data and to non-automated processing of personal data contained in or intended to be contained in a filing system and is therefore corresponding to the old article of the Directive.

The exceptions also remain almost the same. Indeed, the Regulation excludes from its scope personal data processing carried out:

(a) in the course of an activity which falls outside the scope of Union law;

(b) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU (i.e., "Specific Provisions on the Common Foreign and Security Policy");

(c) by a natural person in the course of a purely personal or household activity;

(d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

Completely different is the situation regarding the territorial scope, which changes significantly from the past. In Directive 95/46/EC, the provisions applied only when processing was carried out in the context of the activities of an establishment of the

data controller located in the EU. In Regulation 2016/679, on the other hand, the application is greatly expanded and Article 3 specifies that:

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

2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

(b) the monitoring of their behavior as far as their behavior takes place within the Union.

The major innovation, therefore, is that the framework applies regardless of whether or not the processing is carried out in the Union. In fact, the scope is also extended to data controllers and processors who are not established in the European Union but process personal data of data subjects located in the EU. This change is not particularly welcomed in those non-European countries, the U.S. primarily, where data protection guarantees are lower than in the EU. Indeed, companies in these states, if they want to continue processing data of data subjects located in Europe, will have to change their behavior and comply with the EU Regulation.

4.1.3 Definitions

Proceeding with the analysis of the articles, Article 4 is found to be devoted to "definitions." Unlike the old arrangement, the new one shows an "obsessive" attention to detail and goes so far as to give definitions of as many as twenty-six terms some of which consist of several sub-paragraphs. In addition, the eight definitions formerly found in the 1995 Directive have also been subject to invariably "restoration" work.

As far as the definition of "personal data" is concerned, it remains identical in the structure of the definition to what was in the Directive and, basically, merely adds some identifying elements. Therefore, in addition to the classic types of elements that make a person "identifiable" such as name, identification number, physical, economic or social characteristics, there are also types of identifiers that are closely related to the technologies that have developed in recent years, such as location data (think of the data transmitted by GPS devices) or elements characteristic of a person's genetic identity. Definitions are then added that introduce new categories of personal data related to a person's biological and genetic sphere. These are: 'genetic data,' 'biometric data,' and 'data concerning health.'

Previously there were three categories of data: personal data, judicial data and sensitive data. The latter included precisely the special categories such as biometric data, genetic data and data concerning health. With Regulation 2016/679, however,

the situation is simplified and there is a single category of data, that of "personal data," which contains all kinds of data without distinction.

The definition of processing also experiences changes. In addition to the classic operations of the 1995 Directive, such as collection, organization, storage and modification, new operations are added, such as structuring, adaptation, use, and finally limitation of processing, the definition of which consists of "the marking of stored personal data with the aim of limiting their processing in the future."

When talking about processing, it is essential to define the two figures of the data "controller" and the data "processor" who are the active parties at the top of the data processing activity. According to point 7 and 8 of Article 4:

- *"controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;*
- *"processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.*

The definition of these two entities does not change much from the previous version although their importance after the 2016 Regulations will grow considerably. More information on these figures will be given later.

On the other hand, the definition of consent of the data subject appears to be expanded where it seems clear that the 2016 legislator wanted to make the requirements for consent as punctual as possible in order for it to be considered validly given, and in order to avoid, as well, dangerous interpretative drifts. In the New Regulation, consent is still presented as a free, specific and informed manifestation of will (as in the Directive), but it must also be unambiguous. In order to prevent consent from being interpreted as presumed, the data subject must therefore manifest his or her assent, and consequently, tacit or passive consent or the pre-selection of boxes cannot be considered "consent."

4.2 THE PRINCIPLES OF THE REGULATION

Chapter II of Regulation 2016/679, which runs from Article 5 to Article 11, is devoted to "Principles."

As if to emphasize even more the centrality that Data Processing assumes in the new discipline, the 2016 Regulation no longer titles the first article "Principles relating to Data Quality" (Article 6 Directive 95/46), but decides to rename it "Principles applicable to the processing of personal data." To make it as clear as possible, Article 5 breaks down the basic principles regarding processing and the qualities that data must possess into six points. Personal data must be:

a) processed lawfully, fairly and transparently with regard to the data subject;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; and

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 purposes for which they are processed, are erased or rectified without delay:

e) kept in a form that enables the identification of the data subjects for a period of time not exceeding the achievement of the purposes for which they are processed; personal data may be kept for longer periods only under certain conditions;

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures;

Furthermore, in the second paragraph of the same article, one of the pillars of the new Regulation, the principle of accountability, emerges:

g) accountability, where it is stipulated that the data controller is the party responsible for compliance with all these principles and that an obligation arises on the latter to prove compliance.

Previously, the minimum-security measures to be taken in order not to incur sanctions were indicated, while the new legislation entrusts the Data Controller with

the choices and responsibilities of the technical and organizational measures to be taken for data protection. The Regulation therefore gives the Data Controller a decidedly more proactive role, with more incisive obligations aimed at ensuring the correct application of the Regulation.

Regarding Article 6, which addresses the principle of lawfulness, no notable differences are presented from Directive 95/46/EC; rather, it is the almost literal transposition.

A significant novelty, however, is Article 7 of the Regulation, "Conditions for Consent," which specifies the conditions under which the data subject can express and revoke consent. Article 7 provides as an obligation on the data controller that where processing is based on consent, the data controller must be able to demonstrate that the data subject has given consent. It is also provided that the data subject shall at any time have the right to withdraw his or her consent freely and with the ease with which he or she has given it, specifying, however, that the withdrawal of consent shall not affect the processing that took place previously.

In the same perspective as the provision just considered is the next article, headed "conditions applicable to the consent of minors in relation to information society services," which is an even more significant new element, since there is no corresponding provision in Directive 95/46/EC. This rule in fact dictates a regime of special protection with respect to minors: data processing is lawful where the minor giving consent is at least 16 years old. Otherwise, consent must be given or

authorized by the holder of parental responsibility.

Several countries have modified this threshold, such as in Italy, (Legislative Decree 101/2018), where the age threshold has been lowered to 14.

4.3 RIGHTS OF THE DATA SUBJECT

Chapter III of EU Regulation 2016/679 deals with "Rights of the data subject." Some rights are better defined than in the past, while others are introduced from scratch. The rights of the data subject represent declinations of the individual's more general claim to be able to project oneself freely into the world through one's own information, while retaining control over the way it circulates and is used, regardless of whether there has been a breach.

First of all, it should be pointed out that the data subject is not a subject who passively undergoes the processing of data, but, on the contrary, he or she has an important power of control over his or her personal data and is entitled to exercise various rights over them. The Chapter opens with the "right to information," which confirms and specifies the right in the previous directive. The data controller must inform the data subject about the processing operations "in a concise, transparent, intelligible, and easily accessible form, in plain and simple language." This is primarily to enable awareness of what may happen to the data and facilitate the data subject's exercise of rights. In addition, information is required to be provided in writing or by electronic means; oral information is permitted under two conditions:

there must be a request from the data subject and the identity of the data subject must be proven by other means.

The Regulations also recognize the data subject's right of access to his or her personal data. The latter thus has the opportunity to exercise effective control over the personal data concerning him or her by obtaining information at any time, both in order to understand whether his or her personal data are to some extent being processed and about the purposes of the processing itself. This right can be exercised in order to then understand what categories of data are involved, the existence of automated decision making, and their retention period. The Regulation introduces important innovations precisely regarding the retention period of personal data. Again in accordance with the principle of accountability, the Data Controller is obliged to indicate the period or criterion of data retention and bases this choice on the purposes for which the data is processed. The Data Controller is obliged to ensure that the period of retention of personal data is limited to the minimum necessary and must be able to justify the chosen timeframe so that the data subjects' right to data protection is not impaired in any way.

In addition, the data controller has an obligation to rectify or supplement inaccurate or incomplete personal data, and this must be done "without undue delay." Article 18 of the Regulation provides that in the four cases expressly provided for by law, the data subject is granted the right to restriction of processing, that is, the right to place unavailability and unusability constraints on his or her personal data. Finally,

it can be said that it is the data subject's right to object to the processing of his or her personal data at any time, for reasons related to a given situation. In particular, the opposition turns out to be a real declaration of will on the part of the data subject, which implies that the Data Controller will have to stop processing permanently, especially when the data are the subject of direct marketing.

4.3.1 Right to erasure (“right to be forgotten”)

Article 17 is undoubtedly one of the most interesting elements of the entire Regulation. It, in fact, regulates the "Right to erasure" of personal data, also called "right to be forgotten' ".

According to the first paragraph of this provision, erasure can be requested and obtained by the data subject in a whole range of situations:

- if the personal data are no longer necessary in relation to the purposes for which they were collected or processed;
- if the consent on which the processing is based is withdrawn;
- if the data subject objects to the processing (based on Article 21, which deals precisely with the "right to object");
- If the data are processed unlawfully;
- if erasure is necessary to fulfill a legal obligation to which the controller is subject;
- if the data have been collected in connection with the provision of information society services.

In these cases, the owner has an obligation to erase the data without undue delay.

The most innovative aspect of the provision, however, is certainly paragraph 2. In fact, where the data controller has made personal data knowable to everyone by disseminating it by way of publication (which happens every day on the Web), he or she is obliged to inform other controllers, who are processing such data, of the data subject's request to delete any link, copy or reproduction of his or her personal data. Finally, Article 17 also has a paragraph 3, which provides that the right to be forgotten does not exist in a whole range of cases, such as where the processing is necessary for the exercise of the right to freedom of expression and information, or for the fulfillment of a legal obligation.

This provision, has as its predecessor Article 12 of Directive 95/46/EC, but it obviously dictates a much more nuanced discipline than the previous legal instruments. The right to be forgotten, was born as a result of the need found following several case law pronouncements. Among these, one of the most important is certainly the Google Spain case of May 13, 2014, which pitted Google Spain SL and Google Inc. against the Agencia Española de Protección de Datos (the Spanish Data Protection Authority) [31]. The Court of Justice ruled following an appeal by a Spanish citizen who had requested the removal of some personal data

[31] Bougiakiotis E., 2016, *"The enforcement of the Google Spain ruling"*

published in a few lines of the newspaper "LaVanguardia Editiones SL" (which appeared on Google) and which he considered to be out of date.

As can be easily guessed, this protection stems from the desire to strengthen, especially in the digital world, the data subject's right to obtain the removal of personal information, the processing of which often, in addition to no longer being justified, may even to some extent harm his or her individual sphere. For this very reason, this is referred to as the "right to be forgotten."

One of the most recent court cases may help to understand even better the application of this right. In 2019, the giant Google clashed with the Commission nationale de l'informatique et des libertés (National Commission on Informatics and Liberty), an independent French administrative regulatory body tasked with ensuring data privacy. The dispute had arisen as a result of a sanction by the latter against Google, which had refused to permanently delete some data, merely removing links to them in countries that are part of the European Union[32]. The IT giant, believing the implemented "geoblocking" mechanism to be sufficient and compliant with the GDPR, then appealed to the Court of Justice, which ruled that search engines are also subject to the deletion obligation (which therefore does not turn out to be "circumventable" in any way), adding that within the European Union the right to privacy may prevail over the economic interest of the search engine

[32] Globocnik J., 2016, *"The Right to Be Forgotten is Taking Shape: CJEU Judgments in GC and Others (C-136/17) and Google v CNIL (C-507/17)"*

operator. However, the Court concedes that outside the Union it is not possible to check the balance of Article 17 with the right to information, so in carrying out its work outside the Union, Google is no longer subject to the obligation to delete data.

4.3.2 Right to data portability

Newly introduced, and therefore deserving of special attention, is the "Right to data portability," addressed in Article 20 of the Regulation.

Data portability takes the form of the right on the part of the data subject to receive in a structured, commonly used and machine-readable format personal data concerning the individual provided to a data controller; the data subject also has the right to transmit data concerning him or her to another data controller without any hindrance from the data controller to whom he or she has provided the data. It is further specified in the second paragraph that the transmission of data from one controller to another, if technically feasible, may be done directly, thus without the data subject having to physically transfer the data. Such a possibility undoubtedly constitutes a considerable saving in terms of economy and speed of procedures. Finally, in the last two paragraphs it is provided that a person's right to portability of his or her data does not in any way affect the operation of the right to erasure provided for in Article 17, and that the right to portability does not apply to those categories of processing necessary for the performance of a task of public interest or otherwise related.

The right to data portability undoubtedly relates closely to the dynamics of the marketplace, the terrain on which it is intended to operate and where data certainly is most susceptible to abuse. So here it is that in a "healthy" market, in order to avoid situations of abuse, the user must be guaranteed the ability to be able to switch services easily, taking his or her data with them from one service provider to another, as is usually the case when changing a telephone provider; this should also be able to be done from one service provider to another, as in the case of social networks. In this way, data would no longer be "hostage" to online service providers, and those who wanted to change providers would be able to take their digital history with them and resume the journey with a new provider exactly where they left off with the old one.

Such a right certainly has a multipurpose function. First and foremost, it allows the data subject to overcome the constraints that bind him or her to the data controller if he or she sees it appropriate; at the same time, since portability allows for a circulation of personal data directly between data controllers, it facilitates the development of information society services, or in other words, their collaboration.

4.4 DATA CONTROLLER AND PROCESSOR

While the rights of the data subject are clearly strengthened, the burdens placed on the controller and processor are also increased: not surprisingly, after the Chapter just reviewed, it is possible to find Chapter IV, devoted entirely to these two figures.

The importance that the legislature places on the rules focusing on the duties of the controller and processor can be guessed from a quick analysis of the regulatory structure.

Indeed, it can be seen that Chapter IV is one of the largest regulatory blocks of the new framework, divided into no less than five sections. The Chapter entitled "Controller and processor" opens with Article 24, which speaks of "Responsibility of the controller." The controller, as described in Article 4 of the Regulation (Definitions), is that entity (natural or legal person, public authority, service or other body) that determines the modalities, purposes and operational choices regarding the processing of data and thus stands at the top of the pyramid of the subjects of processing. Article 24 expressly provides that the controller shall take appropriate technical and organizational measures so as to ensure, and be able to demonstrate, that the operations put in place by him or her during the processing comply with the provisions of the Regulation. The controller shall put in place such measures only after having assessed the nature, scope, context and purposes of the processing, as well as having first probed what the risks, in terms of likelihood and severity, to the rights and freedoms of natural persons are. In the last paragraph it is also provided that adherence to codes of conduct (Art. 40) and/or certification mechanisms (Art. 42), can be used by the data controller as an evidence to demonstrate compliance with obligations and the conformity of its actions with regulatory provisions. Thus, a center of imputation of responsibility carved out on the figure of the data

controller appears to be more delineated. The legislator, on closer inspection, seems to opt for an approach geared not to the reparation of the wrongdoing, but to that of the prevention of damage; this would also be confirmed by the fact that the provision lacks an exhaustive list of the tasks and activities that the data controller must put in place, but rather preference is given to the analysis of the risk and of the possible damage caused, whereby the controller is obliged to put in place "appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation" (Article 24 (1)).

The Regulation also regulates the case of co-ownership of processing, i.e., that case whereby two or more controllers jointly determine the purposes and means of processing. Co-processing, however, is not synonymous with equal responsibility among the Controllers. Co-owners, in fact, are required to draw up a written agreement in which each of them delimits its responsibilities regarding the processing it puts in place, in pursuit of a single common objective: the protection of the rights of the data subject. Finally, it should be kept in mind that the data subject can exercise his or her rights vis-à-vis each Data Controller, also having the opportunity to view the essential content of the agreement that binds the Data Controllers.

The Data Processor, on the other hand, is identified, again according to Article 4, as the "natural or legal person (...) which processes personal data on behalf of the

controller." The processor is configured as a contingent entity in the sense that the controller uses the services of the processor if it is indispensable and the processing "must be carried out on behalf of the controller." In this regard, Article 28, in its first paragraph, specifies that the controller shall only use the services of those processors who present sufficient guarantees to put in place that set of technical and organizational measures that are appropriate for the fulfillment of regulatory requirements and the protection of the rights of data subjects. It is also provided that the relationship between the controller and the processor, as well as the processing by the latter, shall be governed directly by a contract or other legal act, concluded in writing, binding the processor to the controller and establishing respectively: the subject matter regulated, the duration, nature and purpose of the processing, the type of personal data and the category of data subjects, and the obligations and rights of the controller.

The data processor therefore has a primarily supporting function with regard to the functions and tasks of the data controller, referring strictly to the provisions of the data controller arising from the contract.

It is also provided in the Regulations that the data processor may use another data processor, subject to specific or general written authorization from the owner. In this case, too, a relationship is established between the data processor and the sub-processor of a contractual nature, as between the data controller and the data processor, having the same contents as the agreement; the only note of distinction

can be found in the event that the other data processor fails to fulfill its specific data protection obligations: in this case, the entire responsibility for compliance will still fall on the initial data processor.

4.4.1 Records of processing activities

In closing Section I, there are two other provisions that refer to obligations of the controller and the processor in Articles 30 and 31. Article 30 provides for the obligation to maintain a record of processing activities. Specifically, the records go to form that documentary apparatus that is mandatory only for companies or organizations with more than two hundred and fifty employees, or if the processing operations carried out by these entities involve special personal data or processing that may present substantial risks to the rights and freedoms of the data subject. This obligation undoubtedly has the purpose, rather than genuine protection of the data subject, of facilitating monitoring by the guarantor authorities, should they request clarifications from data controllers regarding the processing operations carried out.

According to the provisions of the Regulation, both the Data Controller and the Data Processor have their own register, the contents of which the legislator indicates in detail. The Controller's record must necessarily contain all of the following information:

(a) the name and contact details of the data controller and, where applicable, the joint data controller, the data controller's representative and the data protection officer;

(b) the purposes of the processing;

(c) a description of the categories of data subjects and categories of personal data;

(d) the categories of recipients to whom the personal data have been or will be disclosed, including recipients in third countries or international organizations;

(e) where applicable, transfers of personal data to a third country or international organization, including identification of the third country or international organization and documentation of appropriate safeguards; and

(f) where possible, the expected time limits for deletion of the different categories of data;

(g) where possible, a general description of technical and organizational security measures.

On the other hand, the processor's record, probably by virtue of the fact that he or she carries out processing on behalf of the Controller, is somewhat simplified, in that it is essential that he or she indicate only in addition to the identification data of the subjects, the categories of processing, transfers and a description of the measures put in place.

Finally, in Article 31 entitled "Cooperation with the supervisory authority," there is a general obligation for the controller, the processor and when provided for of their

representative, to cooperate with the supervisory authority in the performance of its tasks, if it so requests. The regulations provide that, if checks are carried out, the Controller and the Processor shall make fully available to the Supervisory Authority the records of processing, which require written form but may also be kept in electronic format.

4.4.2 Privacy by design and by default

Still on the level of new obligations, which especially burden the data controller, Regulation 2016/679 introduces two very important principles stated in Article 25. Commonly referred to as "privacy by design" and "privacy by default," but the Regulation reads "data protection by design and by default."

The first of the two principles (privacy by design) is enshrined in paragraph 1, which requires the data controller to put in place appropriate technical and organizational measures aimed at effectively implementing the data protection principles; and this is not only at the stage of the execution of the processing, but from the time of the design of the processing.

The principle of privacy by default, on the other hand, is affirmed by paragraph 2: the controller must implement appropriate technical and organizational measures to ensure that only the personal data necessary for each specific purpose of processing are processed by default. These measures must specifically ensure that, by default,

no personal data are made accessible to an indefinite number of individuals without human intervention. It should be noted that protection by default covers:

- the amount of data collected;
- the extent of processing;
- the retention period;
- accessibility.

The scope of these two principles should by no means be underestimated. Indeed, in this way, a proactive approach is imposed on businesses as well as public administrations: data protection is now a real strategic asset, to be evaluated beforehand, already at the design stage of new procedures, products or services.

4.4.3 Security of processing and data breach

The Regulation devotes Section 2 of Chapter IV to "Security of personal data." According to the provisions of the Regulation, a personal data breach consists of a "breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed" (Art. 4 par. 12).

On this topic, the Supervisors have outlined three types of violations[33]. The first is defined as "breach of confidentiality," in the case of unauthorized or accidental

[33] Liu F., Cheng L, 2017, *"Enterprise data breach: causes, challenges, prevention, and future directions: Enterprise data breach"*

disclosure of or access to personal data; the second as "breach of integrity," in the case of unauthorized or accidental modification of personal data; and the last as "breach of availability," in the case of accidental or unauthorized loss, access or destruction of personal data. At this point one can well imagine that in the context of personal information, the harm is not limited to the breach as such, but to the misuse that may result. For this reason, with the adoption of the Regulation, the legislature has provided that whenever a Data Controller suffers a breach of security measures, he or she must first notify the Supervisor in a timely manner; Article 33 of the Regulation provides precisely for the notification procedure to the Supervisory Authority. Specifically, if there is a Data Breach, the Data Controller must notify the Supervisory Authority of the breach within 72 hours of becoming aware of it, unless the personal data breach is unlikely to present a risk to the rights and freedoms of individuals. If the notification to the Guarantor is not made within 72 hours, it must be accompanied by the reasons that generated the delay.

In the following article, on the other hand, the legislator stipulates that if the breach may pose a high risk to the rights and freedoms of the person, the Data Controller is required to notify the data subject of the breach without undue delay so that the data subject can take all necessary precautions. Such notice must contain at least the contact details of the Data Protection Officer or other point of contact, describe the hypothetical as well as likely consequences of the breach, and describe the measures taken or proposed to be taken to remedy the breach. The notice also

should be expressed in plain and clear language that allows the data subject to best understand the nature of the breach. In contrast, although the risks generated by the breach are high, the controller is not required to notify the data subject in cases where:

a) the controller has implemented appropriate technical and organizational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorized to access it, such as encryption;

b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;

c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

Finally, where the Controller has decided not to give notice to the data subject, the Supervisory Authority, after assessing the level of risk arising from the breach, has the power to require such compliance from the Controller or may simply find that one of the above conditions has been met.

4.4.4 Data protection impact assessment and prior consultation

The goal of the European legislature to raise the bar of personal data protection takes a further step forward in Section 3, thanks to the introduction of two very important institutes, which emphasize even more the importance of preventive and precautionary rather than subsequent-reparative protection. Impact assessment and prior consultation configure a protection of personal data devoted to pragmatism, in that it becomes an obligation to carry out these activities in order to comply with the principles of processing, and devoted to dynamism, in that these are fulfilments that, by their very nature, must update, whenever processing operations develop.

According to Article 35 of the Regulation, the controller shall carry out an impact assessment before processing, if a particular type of treatment poses a high risk to the rights and freedoms of persons, taking into account the fact that within the proceedings the use of particular new technologies is envisaged, and considering in addition the context, nature, object and purpose. It is provided that during the conduct of the assessment, if it is designated by the organizational chart of the holder's structure, the data protection officer is involved as a professional subject, acting as a technical advisor[34]. The impact assessment is configured as a fundamental and unavoidable step of all those very risky forms of processing, among which, by way of example, Article 35(3) identifies the systematic and

[34] Schiering I., Friedewald M., 2020, "*The Data Protection Impact Assessment According To Article 35 Gdpr"*

comprehensive assessment of personal aspects of natural persons through automated processing, including profiling, and on which decisions are based that have legal effects on said persons; or the large-scale processing of categories of so-called sensitive personal data; and finally, the large-scale systematic surveillance of an area accessible to the public. In addition, in order to facilitate the task of the controller both in the assessment and in the subsequent stages, supervisory authorities may draw up lists in which the types of processing for which a pre-impact risk assessment is necessary, or not necessary, are enclosed and explained. Finally, as regards the minimum essential content of the assessment, this is regulated in paragraph 7, which stipulates the necessary presence of at least:

(a) a systematic description of the intended processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the data controller;

(b) an assessment of the necessity and proportionality of the processing in relation to the purposes;

(c) an assessment of the risks to the rights and freedoms of data subjects;

(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned.

In the immediately following provision, on the other hand, it is stipulated that whenever the impact assessment reveals a real high risk, in the absence of appropriate measures to mitigate the risk, the controller, before proceeding with the processing, must compulsorily consult the supervisory authority. The latter, if the processing is found to be unlawful or deficient in terms of adequacy for the prevention of the risk, has the burden of providing a written opinion within eight weeks of the request for consultation (extendable by an additional six weeks, with the respective obligation to inform the owner) with the power to exercise the investigative, corrective, authorizing and advisory powers provided for in Article 58 of the Regulation. For the purpose of drafting the written opinion, the holder shall, in order to make the overview of the situation complete to the supervisory authority, inform it of:

(a) the respective responsibilities of the data controller, the co-processors and the controllers, in particular with respect to processing within a business group;

(b) the purposes and means of the processing;

(c) the measures and safeguards provided to protect the rights and freedoms of data subjects ;

(d) the contact details of the data protection holder;

(e) the findings of the impact assessment referred to in Article 35;

(f) any other information requested by the supervisory authority.

4.4.5 Data protection officer

The last figure that emerges within Regulation 2016/679, and perhaps one of the most impactful innovations, is the Data Protection Officer (DPO) covered in Articles 37, 38, and 39, in Section 4 of Chapter IV.

It should be pointed out that the figure of the DPO does not represent an absolute novelty. Although previous privacy legislation did not include specific obligations in this regard, in more complex organizations the presence of a figure with the objective of protecting personal data was almost a practice. Instead, following the adoption of the Regulations, Data Controllers and Data Processors who meet certain requirements are obliged to appoint a Data Protection Officer. Specifically, the Regulation provides for the mandatory appointment of a DPO in three cases:

a) if the processing is carried out by a public authority or public body;

b) if the main activities of the controller or processor consist of processing that requires regular and systematic monitoring of data subjects on a large scale;

c) if the principal activities of the controller or processor consist of large-scale processing of special categories of data or personal data relating to criminal convictions and offenses.

The interpretation of some parameters, however, is not straightforward, so the contribution offered by the European Supervisors through the Guidelines on Data Protection Officers issued on December 13, 2016, is really valuable. For example, the Regulation does not offer a definition of "large-scale" processing, but an attempt

has been made to fill this gap by recommending that certain factors be taken into account when determining whether or not a processing is carried out on a large scale, such as: the number of data subjects affected by the processing, the volume of data and/or the different types of data being processed, the duration of the processing activity, and, lastly, the geographic scope of the processing activity.

Some companies, despite the fact that they are not obliged by the legislation, decide on a voluntary basis to designate a Data Protection Officer anyway. In addition, it is certainly appropriate for Controllers and Processors to document the assessments made that did or did not lead to the appointment of such an individual.

Companies that are part of the same business group, nationally or across borders, may appoint a single DPO, as long as he or she is easily accessible from each establishment. Something similar to what has just been stated is also provided for public entities: in fact, it is possible to appoint a single DPO for several public authorities or public bodies, taking into account their organizational structure and size.

The Data Protection Officer, is designated on the basis of professional qualities, but above all on the basis of specialized knowledge of data protection regulations and practices. As can be easily inferred from Article 37 of the Regulation, it must have significant legal skills but must also work with IT professionals, seeking to implement regulatory standards within information systems. It is not necessary that he/she be an employee of the Data Controller or Processor, but it is essential in

order to maintain a certain degree of independence that he/she does not receive any instructions on the tasks to be performed and reports directly to the hierarchical top management of the Data Controller or Processor. In fact, this figure, who acts almost as an "internal guarantor," is a decisive junction for the purposes of the already mentioned principle of "accountability."

In terms of functions, the Regulation assigns the Data Protection Officer the task of:

- informing and advising the controller or processor as well as the employees carrying out the processing about the obligations arising from this Regulation as well as from other Union or Member State provisions relating to data protection;
- oversee compliance with this Regulation, other Union or Member State provisions relating to data protection as well as with the policies of the controller or processor relating to the protection of personal data;
- provide, if requested, an opinion on the data protection impact assessment and monitor its conduct in accordance with Article 35;
- cooperate with the supervisory authority;
- act as a point of contact for the supervisory authority for matters related to the processing, including prior consultation (Article 36), and carry out consultations, where appropriate, regarding any other matter.

In addition, data subjects may contact the DPO for all matters related to the processing of their personal data and the exercise of their rights under this

Regulation. The DPO shall report directly to the top management of the controller or processor. This means that the DPO will interface directly with the CEO or otherwise with the company's top hierarchy, without intermediate steps. Therefore, we are dealing with an autonomous and independent person who will have great depth in the company's organization. However, it should be pointed out that this figure is not personally liable in the event of non-compliance with the provisions of the Regulation; in fact, the Data Controller and the Data Processor are the only ones who have the burden of proving that all the measures taken comply with the Regulation itself. Finally, the Data Controller or the Data Processor must facilitate the DPO in the performance of his or her duties and are therefore required to provide him or her with all the necessary resources, including full access to personal data and the processing operations implemented.

4.4.6 Codes of conduct and certification

Having completed a general description on the DPO, the codes of conduct and certifications regulated in the last section of Chapter IV also deserve mention. Paragraph 1 of Article 40 provides that "*The Member States, the supervisory authorities, the Board and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises.*"

Drawing up, amending or extending these codes for the purpose of specifying the application of the Regulation are associations and other bodies representing categories of data controllers or processors. The draft codes, like the modifications and extensions, are submitted to the supervisory authority, which gives an opinion on compliance with the Regulation and finally approves, if it considers that adequate guarantees are offered to a sufficient extent. In addition, under certain conditions, the Commission may decide by means of implementing acts that certain codes of conduct submitted to it have general validity within the Union, and the same applies to amendments and extensions.

A mention should be made of Articles 41, 42 and 43. The first of the three regulates the mechanism for "monitoring codes of conduct," but the real novelty is in Article 42, which speaks of "certification" mechanisms.

This certification, which is voluntary and accessible through a transparent procedure, is issued by special bodies regulated in Article 43 or by the monitoring authority for a maximum period of three years, and can be renewed, but also revoked, before expiration. It should be emphasized, however, that certification does not reduce the responsibility of the data controller and data processor with regard to compliance with the Regulation and is without prejudice to the duties and powers of the supervisory authority.

4.5 TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

Regarding the transfer of data to third countries and international organizations, which is governed by Chapter V (Articles 44-50), it should be emphasized at the outset that Regulation 2016/679 leaves fundamentally unchanged the approach already enshrined in Directive 95/46/EC, although it is more detailed and strengthened.

The GDPR ensures the possibility of transferring data to states that are outside the EU, as long as these states guarantee an adequate level of protection. To assess adequacy, Article 45(2) lists what criteria guide the adequacy assessment. The list includes parameters that are analyzed for the assessment of the third country or international organization, such as "the rule of law, respect for human rights and fundamental freedoms, relevant legislation, data protection rules, professional rules and security measures, case-law etc."

In addition, Member States and the Commission shall inform each other of cases where, in their opinion, a third country does not provide an adequate level of protection. If the Commission finds that a non-European state does not ensure an adequate level of protection, EU countries must take all necessary measures to prevent data transfers to that state. The adequacy decision, which is made by the Commission through implementing acts, is subject to periodic review (at least every

4 years), taking into account all developments. In addition, where it deems it necessary, the Commission may revoke, modify or suspend the adequacy decision. Even if the adequacy decision is not approved, the transfer can still be made, but under certain conditions. Article 46(1) provides that the controller or processor may transfer personal data to a third country or international organization only if it has provided adequate safeguards and provided that data subjects have enforceable rights and effective remedies. What are adequate safeguards is specified in paragraph 2 of the same article. By way of example: binding corporate standards, model contract clauses, codes of conduct, approved certification mechanisms etc. Finally, Article 49 contains "exceptions in specific situations," which allow the transfer while lacking both the adequacy decision of Article 45 and the adequate safeguards of Article 46. These exceptions, however, include cases where: the data subject has explicitly consented to the transfer; the transfer is necessary for important reasons of public interest; the transfer is necessary to establish, exercise or defend a right in court; and the transfer is necessary to protect the vital interests of the data subject or other persons.

4.6 INDEPENDENT SUPERVISORY AUTHORITIES

One area that has been enormously reformed is certainly that concerning the Independent Supervisory Authorities (Chapter VI Reg.), which has significant differences from the past. These figures are at the heart of the supervision and

proper application of the Regulation in a uniform manner throughout the Union, and their importance has increased considerably over the years.

As a general rule, it is provided that each member state has one or more independent public authorities in the territory (Article 51) and that the authorities act freely and independently, not having to be subject to any kind of external pressure, direct or indirect, in the performance of their duties and in the exercise of their powers. The duties incumbent on a supervisory authority in its territory are listed in a long list in Article 57. These include: supervising the correct application of the regulation, promoting awareness of risks related to the protection of personal data, carrying out advice for institutions, promoting awareness among data controllers of their obligations and duties, providing information at the request of data subjects regarding the exercise of their rights etc.

Each authority has the ability to exercise three groups of powers: investigative powers (enjoining the data controller to provide it with all kinds of information), corrective powers (issuing warnings to the data controller or processor), and authorizing and advisory powers (providing advice to data controllers or other institutions).

Finally, it is worth mentioning another important innovation consisting of the introduction of the European Data Protection Board. The Committee is established as a body of the European Union, with legal personality, represented by its chairman and composed of the top figure of each supervisory authority for each member state

and the European Data Protection Supervisor. The Committee's main objective is to ensure the consistent application of the Regulation through the publication of guidelines, recommendations, opinions and best practices. It also advises the Commission on formats and procedures for exchanging information between data controllers and supervisory authorities, or for assessing the adequacy of the level of protection of a third country or international organization.

4.7 THE TIGHTENING OF THE LIABILITY AND PENALTY SYSTEM

In conclusion, the major change in perspective adopted by EU Regulation 2016/679 is undoubtedly that of having centered the new system entirely on the figures of the Controller and Processor and the profiles of the latter's obligations and duties. The discipline therefore no longer focuses exclusively on the rights of the data subject, but the protection, in an explicitly preventive and precautionary perspective, necessarily passes through a careful elaboration of each phase of data processing (especially security measures) before it is put in place.

The civil liability regime elaborated by the Regulation, is anything but smooth for the data controller and data processor who, under Article 82, are liable for any material or immaterial damage caused by a violation of the Regulation following,

upon the establishment of such a violation, the right to compensation in favor of the data subject who suffered the damage.

As far as the sanctioning apparatus is concerned, there have been no relevant novelties, but certainly the Regulation, deciding to value the dangerousness of the processing activity and the seriousness of injury to which the personal data of individuals may be subjected, has opted for a decisive tightening of the sanctioning regime, listing punctually the modalities, conditions and amounts of disbursement[35].

According to Article 83, it is the competent supervisory authority to impose and determine the amount of the administrative penalty, provided that the fine is in each individual case effective, proportionate and dissuasive. Indeed, it is striking to note the wide margin of discretion that the European legislator entrusts to the supervisory authority in assessing the whether and quantum of the penalty, an assessment that in each case will have to take into account, on a case-by-case basis, certain elements such as:

- the nature, gravity and duration of the violation;
- the intentional or negligent nature of the violation;
- the measures taken by the data controller or processor to mitigate the harm suffered by the data subjects;

[35] Bouthinon-Dumas H., Voss G., 2021, *"EU General Data Protection Regulation Sanctions in Theory and in Practice"*

- the degree of responsibility of the data controller or processor;
- the categories of personal data affected by the breach;
- adherence to codes of conduct or certification mechanisms.

In the event of a violation of the provisions concerning the obligations of the controller or the obligations of the certification body or the control body, the supervisory authority may impose an administrative fine of up to 10,000,000 euros or, for enterprises, up to 2 percent of the total annual worldwide turnover of the previous fiscal year, whichever is higher. On the other hand, "more serious" sanctions are envisaged if provisions concerning the basic principles of processing, conditions of consent and rights of data subjects are violated; transfers of personal data to third countries or to an international organization. For these violations there are more severe fines of up to 20,000,000 euros and up to 4 percent of the previous annual worldwide turnover, whichever is higher, for companies.

Once again the shift in perspective of the data protection regulations from Directive 95/46/EC is noticeable. The Regulation aims to severely sanction unlawful processing, in a far broader perspective than the dimension of the individual, striving for a comprehensive protection of subjects from unlawful processing, especially when the relevant number of data processed or the particular type of proceedings integrate collective risks of significant size and scope.

The GDPR can certainly be seen as a benchmark from which to ensure a higher level of transparency and security in the processing of personal data, promoting the protection of the rights of data subjects and strengthening European citizens' confidence in technological progress.

At the same time, this regulation can be an inspiring launching pad for kick-starting corporate reorganization projects that will lead to a reorganization of processes, better management of digital and paper archives, and pave the way for an inevitable process of digital transformation.

It may be useful to see the GDPR not only as a set of instructions for the proper protection of personal data, but also as a guide toward a more ethical, modern, profitable, and secure business model.

Chapter 5

IMPACT OF THE GDPR ON THE ITALIAN COMPANY TOD'S S.P.A.

5.1 INTRODUCTION

The GDPR has revolutionized the world of personal data protection by introducing and rewriting the rights of the data subject and the duties to be fulfilled by those who process personal data. If we would like to see EU Regulation No. 2016/679 as a mountain, it could be said that companies, thanks to this content, are able to descend down its very steep (and sometimes slippery) slopes to safely reach the valley, safe from all the pitfalls of the path to compliance with the new legislation. But what actual impact has GDPR brought to business environments? How have they had to adapt so as not to risk receiving sanctions from regulators? How have non-European countries reacted to the stringent regulations? Is the GDPR still up to date?

To try to understand this and know the real impact the regulation has had, the case of the TOD'S S.p.A. business is examined.

TOD'S Group's Data Protection Officer, Alessandro Reni, was available to help understand the company's internal management of personal data protection and

unravel doubts and concepts that are often complex in order to understand the application of the 2016 Regulation in practice. Mr. Reni has been TOD'S DPO since May 2018 when the GDPR came fully into effect.

Before going to analyze the impact of the GDPR on the company, it is important to have a general overview of TOD'S S.p.A so as to understand what kind of company we are dealing with, its size, businesses around the world, and anything else that may be useful to better understand how it relates to the personal data of data subjects.

5.2 TOD'S S.P.A.

TOD'S S.p.A., (from italian: joint stock company) is an Italian firm specializing in the production of luxury footwear, clothing and accessories under the Tod's, Hogan, Fay and Roger Vivier brands.

It all began in the early 1900s, when Filippo Della Valle, created a small shoe workshop in Casette d'Ete, a small village in the province of Fermo, Italy. The work and passion were passed down to his sons, who gave birth to the footwear business of excellence that has been the Group's hallmark ever since. Della Valle's idea was to create a shoe suitable for both dress and informal occasions, with a casual flavor, comfortable but still refined. In the late 1960s his son Dorino founded, helped by his wife, the first artisan company in Sant'Elpidio a Mare. In the 1970s Dorino's son

Diego also joined the company, and in 1986 he was officially appointed managing director of TOD'S S.p.a., which soon grew from a small family business into a luxury brand in the footwear and leather goods sector. Even today Diego della Valle is the CEO and chairman of the company. After launching the Hogan brand, TOD'S began its international expansion in 1987 with the opening in New York of its first direct store in the United States. Building on the consolidation of the market success of its products in Italy, TOD'S gave further impetus to its strategy of expansion into foreign markets by opening its first boutique in France in 1993 in Paris and, subsequently, in several European markets including in England in 2000. Having consolidated its presence in European markets, the Group started to penetrate Asian markets with the opening of its first store in Hong Kong in 2000 and then in Japan and China in 2002 and 2008, respectively. Expansion into new markets has continued in the last four years with the opening of direct stores in Australia in 2018, Canada in 2019, and the United Arab Emirates in 2021.

The prestige of the brands distributed and the high level of specialization required to present the relevant products to customers make it essential to operate, at the distribution level, through a network of highly specialized stores. To this end, the Group mainly relies on the following distribution channels: directly operated stores (DOS), the e-commerce channel, franchised outlets and a series of selected independent multi-brand stores. There are currently 420 boutiques worldwide, of which 273 are in Asia and 119 in Europe. The stores are conceived as eclectic

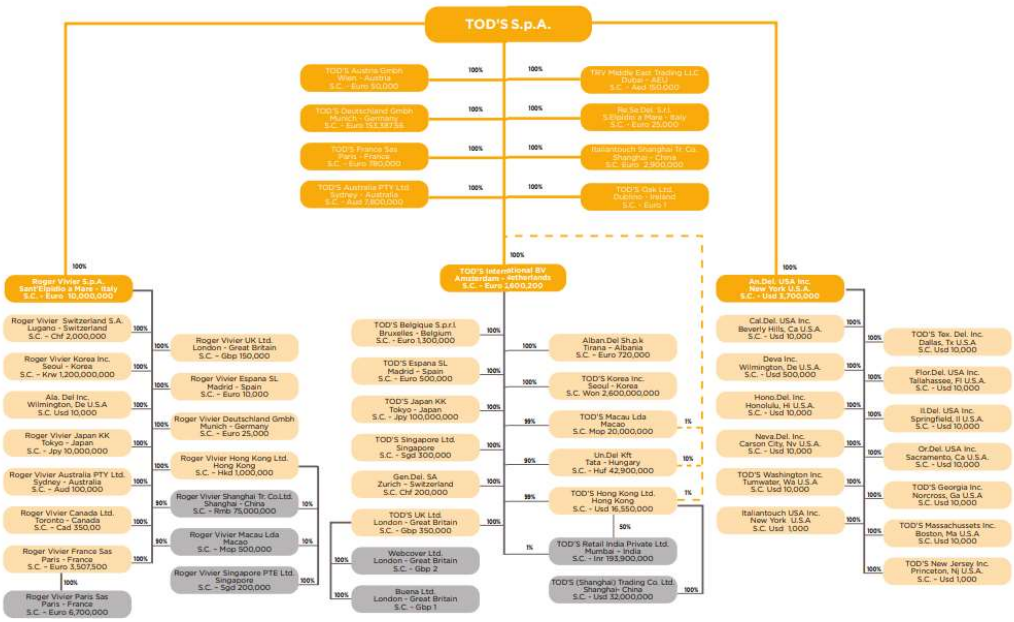
places, where each product is enhanced and each customer is welcomed in an exclusive way; a rich network and well-distributed, capable of bringing the best of Made in Italy to an international level. The e-commerce channel, in particular, is assuming, consistently with the rapid dynamics of the sector, an increasingly central role in the Group's distribution strategy, with the presence of the Group's brand e-commerce sites in 35 countries around the world. The online sales channel and that of directly operated stores, moreover, are rapidly evolving towards an "omni-channel" concept, in which the commercial and distribution interrelationships of the two channels make it possible to offer innovative services and to have a privileged and direct contact with the customer, in order to meet their expectations and build lasting and trusting relationships.

The latest annual report dating back to December 31, 2021 shows that TOD'S can count on 4746 employees of whom 74% are white-collar, 25% blue-collar and less than 1% managers[36].

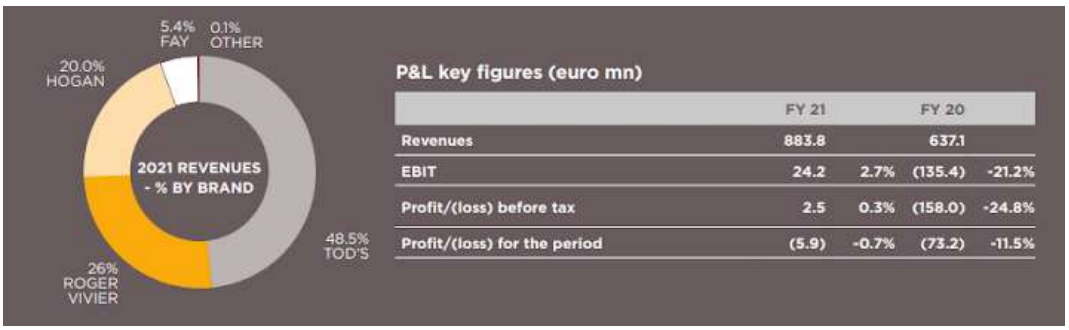
The multinational corporation has a rather complex structure; control is centralized in fact it is always the parent corporation TOD'S to which the various sub-holdings and companies scattered around the world answer and refer. To get an even clearer idea here is the organization chart of the company.

[36] TOD'S, 2021, *"Annual Report TOD'S S.p.A."*

GROUP'S
ORGANIZATIONAL CHART



Although the company suffered greatly from the impact of the Covid-19 pandemic, the situation in the past year seems to have almost recovered to pre-pandemic levels. The Group's consolidated sales in 2021 amounted to 883.8 million euros, marking a 38.7 percent increase over the previous fiscal year 2020 figure, when it was 637.1 million euros, and has almost entirely recovered to the levels recorded before the arrival of the virus (-3.5 percent compared to 2019).

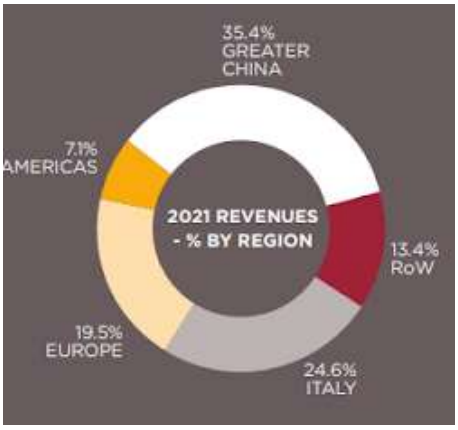


P&L key figures (euro mn)

	FY 21		FY 20	
Revenues	883.8		637.1	
EBIT	24.2	2.7%	(135.4)	-21.2%
Profit/(loss) before tax	2.5	0.3%	(158.0)	-24.8%
Profit/(loss) for the period	(5.9)	-0.7%	(73.2)	-11.5%

On the merchandise category front, sales figures confirm the footwear category as the Company's core business, with FY2021 revenues amounting to 403.3 million euros (305.4 million euros, as of Dec. 31, 2020), accounting for 76.4 percent of total revenues. This is followed by revenues from leather goods and accessories and finally clothing.

The Group's revenues have returned, in particular, to levels close to pre-pandemic levels, driven, above all, by the performance of the TOD'S and ROGER VIVIER brands, which are characterized by a greater presence in Asian markets and, above all, in Greater China. In these markets, the Group has, moreover, further strengthened its direct distribution network, with several new openings, during the fiscal year, especially in South Korea and Mainland China, which will help provide further impetus to growth.



The company is majority owned by the founding Della Valle family and has been listed on the Italian Stock Exchange in Milan since 2000 and is part of the FTSE Italia Mid Cap index.

5.3 GDPR COMPLIANCE PROCESS

"The TOD'S Group presides over privacy-related issues in an organic and structured manner and has adopted appropriate organizational, operational and technological measures in order to ensure compliance with the provisions of European Data Protection Regulation 679/2016."

Two years passed between the date of publication of the GDPR in the European Official Journal on May 4, 2016 and its actual implementation on May 25, 2018, a time when companies, organizations and institutions had to revise several internal processes in order to meet the requirements imposed by the new Regulation.

The TOD'S Group, being a very complex and developed business in many countries around the world, sought assistance from external consultants who could follow from start to finish the whole process of GDPR compliance. For Italy, the country where the head office of the holding company is based, reference was made to one of the big four that dominate the audit and consulting market: Deloitte & Touche S.p.A.

Whether or not to engage an outside consultant is a decision for the company and depends greatly on the size and structure of the company. The advantage of relying on a consulting firm is that it certainly has a qualified and valid methodology and in-depth knowledge on the subject, however, there is a risk that the consultant, not being fully familiar with the company's operations and internal management of all

processes, may not be able to meet all needs and may not find the most effective way forward. This is why a trait d'union is needed between a correct methodology, offered by the consulting firm, and the in-depth knowledge of the company's dynamics that only those who work internally within the company can give. In the case of TOD'S, a figure similar to the DPO was appointed to follow the compliance process working closely with the external consultants.

The compliance process requires money and time, which is why two years were made available before the actual implementation of the GDPR. As far as the economic cost is concerned, an investment to come into compliance is mentioned, which can be around 80,000 euros if the company is of modest size up to even 250,000 euros in the case of more developed companies or those operating with a larger amount of personal data. In the case of TOD'S the investment has been around 200,000 although it is very difficult to define a precise estimate.

On the other hand, with regard to the time it took to comply with the new Regulation, it is hard to imagine that it took less than six months to come into compliance, and most companies, as well as TOD'S itself, took approximately 9 months before they had updated and innovated all their business dynamics. Although compliance with the GDPR could have been started as early as May 2016, TOD'S and the majority of interested parties (to make an estimate about 90 percent of companies) started complying with the new Regulation from the second half of 2017. In doing so, however, about 12 months were available to undertake and

complete all the necessary measures, and once the most challenging ones were completed, there was still time available for the final adjustments (fine tuning). it is important to emphasize that compliance with the data protection rules is an activity that practically never sees an end. It is difficult to work part time in this area in fact GDPR is only the tip of the iceberg. After May 2018, a series of other regulations, opinions of guarantors, positions of the EDPB (European Data Protection Board) or laws were added underneath that even if they did not strictly concern privacy, went to impact the management of personal data. For example, during the pandemic period, many regulations were enacted regarding the processing of workers' health data and thus increased the amount of work that, those in charge of personal data protection have to do. Privacy management is a day-by-day affair that depends on what the various guarantors decide. Each guarantor in addition has its own issues to which it is more attached and on which it legislates more: for example, the French guarantor is very interested in the management of cookies, the Italian one pays a lot of attention to consent, the English one gives a lot of importance to data breaches... Since this is not a stable regulation but one that is constantly evolving, it is difficult to say how long it took or how much money it took to comply with the GDPR since an end point is never reached.

The GDPR has given a big shakeup to companies that have had to rethink many business processes to confrom to the law. This compliance can be seen as a bureaucratic slowdown or as an investment for the future to update the company to

make it more competitive in the global market and more reliable for customers. The GDPR was an opportunity for TOD'S to modernize several internal processes and adjust to standards that could only enrich its business. It had been years since the company had to review internal privacy management, in fact even previously there were laws regulating these issues but since they were not always mandatory or the penalties were almost negligible, most companies had not moved forward for several years. For example previously there was Law 196 of 2003 on personal data but no company considered it. A moment of brilliance occurred in 2008/2009, when there was a proposal for a law to include privacy offenses within a legislative decree, and many companies undertook the rush to comply since noncompliance with privacy fell under the offenses. However, many protests were raised from companies and it ended up that the penalties were so low that the cost of compliance was often higher than the eventual penalty. In 2016 everything has changed since the penalties are much heavier and more checks are carried out, and all companies as a result have had to bring their businesses into compliance.

In addition, any entity that wants to trade and have relations with European citizens must conform to the GDPR and reach its standards. This can discourage foreign companies since the process is quite burdensome and trading with Europe can become more difficult. TOD'S has had the advantage of having all companies around the world reporting to the holding company, TOD'S S.p.A. headquartered in Italy, and thus holds the reins. Since they are all subsidiaries and TOD'S S.p.A is

the data controller, the governing law for all companies in the TOD'S group is the GDPR. A distinction must be made here to better understand which legislation is the reference legislation and what changes have occurred.

For example, if it involves sales through third-party vendors, the GDPR has not made major changes since the main company will not directly process the end customer's personal data. TOD'S sells worldwide primarily on a B to B basis, and so even after 2016, no major changes have occurred as the legislation has focused more on the rights of the end consumer. On the other hand, for sales to final consumers, B to C mode, the ownership of the boutiques is with the local companies in fact they are the ones who invoice, the customers are theirs and the revenue goes on their income statement. So the governing legislation for sales is local. Take the example of an Australian boutique: the processing of customer data used to follow up on contractual fulfillments are the Australian company's. Therefore, the laws are the local ones and GDPR does not matter. This requires a cut-and-paste activity that goes to fill in what European legislation has not already provided for and therefore where foreign limits are stronger than the GDPR.

5.4 DATA PROTECTION OFFICER

Having a direct discussion with TOD'S Data Protection Officer, Alessandro Reni, was an opportunity to better understand how this figure operates within the company, with whom he relates, and the major difficulties he may face.

Most of the people who become DPOs have worked mainly within legal studies followed by about 30 percent who work in the IT (Information Technology) sector. Mr. Reni, on the other hand, described himself as a "white fly" expression that in Italian identifies a person with special characteristics compared to his peers, making him an extremely rare case. In fact he pursued purely economic studies (degree in economics and business) and then specialized in compliance, internal audit and only finally in GDPR compliance. For the last 5/6 years he has dedicated himself completely to GDPR since among the various regulations this one is really invasive and it is impossible to work part time especially in a company as large as TOD'S. Currently within TOD'S he works alone, he does not have a team following his work but the idea is to be joined by at least one other employee in the coming years. The biggest difficulty for the DPO is not so much compliance with the GDPR in the Europe-on-Europe case, so when the company goes to implement processes within European borders, but in the Europe-on-extra-Europe case and then the relationships with all the foreign countries that have different regulations. During the two years following the implementation of the GDPR, the situation was still quite easy. Since the Regulation was pretty stringent it was enough to do iso GDPR

and apply its principles in any country and bad you went in abundance with respect to local regulations. Since late 2019/early 2020, however, this approach is no longer sustainable as many other countries have also started Iso GDPR updates. This means that the structure is similar to the GDPR but each country has then developed, deepened and legislated in various aspects that differ from the European regulation. For example China, late last year, passed the PIPL (Personal Information Protection Law) which has a similar structure to the GDPR but they focused much more on security systems, data transfers outside of China. In fact, the Chinese government rather than focusing on the privacy of citizens has decided to focus on greater control and therefore has raised the barriers for data export. If one only complies with the principles of the GDPR then one cannot comply with Chinese regulations as well.

For large groups and their DPOs therefore, the most difficult challenge is to combine GDPR with the legal regulations applied locally outside the EU, and this is a task that as mentioned takes time and money. The TOD'S group to do this cannot afford to hire a data protection person for every country where it trades and opens a retailer. Besides being very expensive, it would also not make sense. What they do then is to rely on local law firms (with many of whom they were already working with before the GDPR was adopted) and work by "difference": taken what the EU Regulation says, are there parts of the local legislation that are conflicting or are they just missing? If there are differences, the situation is analyzed and what

is needed to balance the different regulations is put in place. This also depends a lot on how data ownership is structured within the company. In some groups for example, the ownership is scattered and there is co-ownership among all the companies. In other groups, as in TOD'S there is central ownership. Then it also depends very much on what kind of personal data is processed, in some cases it is not possible to choose: staff data of local companies are of the local companies not of the owner. On the other hand, for data processed for marketing or profiling purposes, for example, there is more choice or the possibility to structure the ownership according to how the company chooses to act; TOD'S for example for these purposes decided to centralize everything.

In addition to the issues that can be created in dealing with non-EU regulations, the DPO must also find time to manage various relationships within the company. There are two major macro families that go behind personal data: the HR (human resources) world and the customer or prospect (possible customer) world. Regarding the personal data of the company's employees, once everything has been mapped, the work is quite stable and under control since there are often no major changes in personnel. More complex, on the other hand, is the world of customers and potential customers especially with regard to marketing and profiling activities where it is essential to have the consent of the person concerned. Simpler, on the other hand, are activities that serve to execute standard client contracts such as billing, customer care, warranty work, etc.

Another aspect that the DPO must pay close attention to is the marketing and especially digital marketing environment. Technologies are evolving very fast and the ways of contacting customers and prospects are changing all the time: if at first it was all based on e-mails or phone contacts now it is necessary to pay attention also to all the social media, the most known ones but also the emerging ones. In addition, great concern is being created by the metaverse that seems to be becoming an ever closer reality in recent years and that will surely have great impacts on the privacy field.

The DPO should be a 3-headed monster operating in 3 different areas: legal, process, and IT. Each company then works in its own way and depending on the structure it can be understood which sector to give more or less importance to. When considering the IT sector there is often a CIO (Chief Information Officer) within the company and sometimes a CISO (Chief Information Security Officer). In TOD'S for now there is also a Cyber Security Manager (CSM), Francesco Pisacane, who is in charge of managing the security of IT systems, outlining a defense plan, monitoring the infrastructure, processes and coordinating the teams in charge. This important figure was added recently after the GDPR provided for a range of security measures based on the level of processing risk. Although there are not only IT security systems, it is also true that today most of the data runs on the information system and for this reason it must be defended in the best possible way. The DPO and CSM work closely together: although the DPO is not directly

responsible for IT security measures, the DPO must ensure that the security measures taken are in accordance with the risk level of each data processing. Therefore, if there were a data breach within the company, the DPO would not be directly responsible. However, it is relevant at this point to do a little background. When problems arise involving personal data, it is important to first understand whether it is a data breach, unauthorized access, malware that has blocked data availability, or other types. If the internal analysis of the incident reveals that there has been an actual data breach, the DPO, the responsible person in the function where the data was potentially breached, the cyber security manager, and the CEO (he is always the one who is accountable in the end) are brought together. These will decide whether the breach poses a potential risk to the data subjects and if it does whether that risk is high or not to make the report to the data guarantor rather than to the data subjects as well. When there is a data breach, the DPO does not respond if there is no particular security measure; the DPO responds if it is challenged that he or she has not done the proper monitoring of security measures. Basically, the DPO has to put down a kind of audit plan, where with the legal representative and the CEO they define what they are going to look at, what controls to do, and propose implementation measures to show that everything was done within their power. If an email is hacked because the password is too simple and the 12 characters have not been set, the responsible party is not the DPO but the cyber security manager who has to point out to the CIO that the robustness of the

password is not correct; then the implementation of the measure is up to the CIO.

Actually, since the current GDPR definition of data breach is very broad, almost any problem with personal data can be considered a breach. What makes the difference then is to understand whether the incident can bring real risks or not and whether it is therefore important to report it. If we look at the statistics, in Italy data breach notifications are very low because companies are very reluctant to make a declaration: if we compare the number of data breach notifications to the authorities per 100,000 inhabitants, Italy is below the European average and only Greece and Hungary are behind. It tends to be better to make one more declaration than one less, but in reality this is not always the case. In Italy it is very unlikely that the guarantor will make a sanction when one has personally declared that there has been a data breach; however, if it has not been reported and it turns out that the company does not have effective security systems in place, then the sanction is quite harsh given that there has been fault and negligence.

TOD'S always notifies the guarantor if there has been a data breach, as these cannot always be avoided and if one has done everything reasonably necessary to protect the data it is difficult for the guarantor to make a sanction. However, if, for example, the data breach is due to a small mistake such as the loss of a USB flash drive from an employee with data inside, or sending an email to the wrong recipient, in these cases you do not necessarily have to make the report if the risk to the data subjects

is low. However, the data breach should still be mapped, and if asked, it is important to specify why the report was not made.

In addition to reporting to the data protection authority if data breaches have occurred, it is possible for the DPO to have other moments of relationship with this authority. Every 6 months this regulator chooses a sector and an area of investigation and performs an audit: for example, it may choose hospitals or call centers and check the proper process of health data protection or marketing consent. On a sample basis the supervisor's check may then come. In addition, a check may come if the guarantor receives complaints from users and thus has a well-founded suspicion that the company is not complying with the principles of the GDPR. For example, data subjects could report that the company is not executing their rights or send complaints in case they receive ads or calls without marketing consent having been given. The Italian guarantor is very focused on marketing consent and has given the biggest sanctions on these issues. For example, Enel Energia, an Italian multinational in the energy sector, was sanctioned for telephone calls without marketing consent on lists of customers acquired from a third-party supplier. This supplier had sold these lists by contractually guaranteeing that they had marketing consent although this was not true. Even if the supplier was therefore at fault, the regulator told Enel that it should not blindly trust the supplier and at least randomly verify that there was this consent. The company was ultimately given a fine of 26.5 million euros. Similar situations have happened for companies

such as Vodafone, Wind, or Sky.

The last case where the DPO has contact with the guarantor is if the DPIA (data protection impact assessment) should be prepared. Especially in cases where the risk is high and therefore the intervention of the guarantor is necessary, companies will still try to consult with the guarantor when all security measures have already been taken so that the risk of the guarantor flunking the assessment is lower.

If data subjects have a problem with the company before reporting to the guarantor, they can report directly to the data protection officer. The email contact of TOD'S DPO is easily found on the website. As Mr. Reni explained, everything comes to this email, especially emails that have nothing to do with personal data. To make an estimate, every year he gets about a hundred emails that he has to respond to since they concern the exercise of the data subject's rights. Most of these requests are about marketing and unsubscribing from newsletters or similar. Since he is the only DPO for the entire corporate group and since the ownership is central, he gets emails from all over the world and in all languages. All requests must be responded to within 30 days and all must be filed in a special register defined by law to keep track.

5.5 DRAFTING OF DATA PROTECTION DOCUMENTS

To understand the internal functioning of the company even better, it is important to identify the processing operations put in place by TOD'S so as to understand in a detailed manner how the company processes, stores, and uses the personal data of data subjects. The TOD'S group has grown a lot in recent years, has under it 4 different brands and 420 boutiques around the world. The processing implemented by the company is therefore very many and each individual area carries out highly diversified activities.

As the Italian firm is a large enterprise with more than 4700 employees, it is required to compile a record of processing activities, which is mandatory for companies with more than 250 employees. As mentioned above, in Tod's, ownership is central: Tod's Spa is the data controller. All foreign companies, on the other hand, are appointed as data processors for data collection on behalf of Tod's and subsequent marketing activity for more local initiatives and local profiling activity is done on behalf of Tod's. For large-scale marketing and profiling purposes Tod's Spa is the controller. This technique is used by about 80% of the world's luxury/retail companies but is not the only one. For example, the Italian luxury company Gucci has opted for co-ownership with all local companies.

The record of processing is the first document the authority asks for if it has to conduct an inspection. This gives a snapshot of the company, what personal data it operates with and how it handles processing/processes. It tends, as in the case of

TOD'S, to have both a hard copy and a digital copy in Word/Pdf ready at all times, which is the first thing the supervisor checks before going deeper and analyzing the information system. Already from the processing record it can be seen whether the principles of privacy by design and privacy by default have been applied.

Although it is compulsory to prepare the record of processing, it is not necessary, according to the legislation, to make this document available to the public, and practically no company makes this document accessible: in this case, in fact, it is better to publish one less thing than one more to avoid problems. The document contains information inherent to the organizational structure and operations of the company that should not be in the public domain such as the technical security measures taken or the treatments with suppliers. However, in addition to the guarantor, the review of the record can also be requested by data subjects, only if information that concerns them personally is contained and only in the part that concerns them. This in fact is part of the data subjects' right of access to data.

Regarding the content to be put within the processing record, Article 30 of the GDPR leaves a lot of freedom without outlining a common standard. There is information that must be put in by law but it is not specified in what manner, under what structure or order, and each company decides for itself how much to make this document detailed or not. TOD'S has decided to divide the record according to the process. For example, there is a section on human resources, which in turn is divided into all the activities that comprise it: recruiting and selection, contracting,

management of contractual relations with the worker, training, and worker performance evaluation. Or the Marketing section is divided into the following activities: data collection, processing, marketing activities, and profiling activities. And so on...

In the record therefore, all the activities that the company carries out are explained, and for each activity the information explicitly required by law is provided. In addition the firm, in order to facilitate easier management and better understanding of the processing conducted, reserves the right to supplement the section with additional types of information. According to the principle of "accountability" in Article 5 paragraphs 1 and 2 of the EU Regulation, the record of processing activities shall be updated periodically.

Two different registers must always be prepared: the data controller's register of processing activities and the data processor's register of processing activities. This second register of the Data Processor is somewhat simplified due to the fact that it performs processing on behalf of the Data Controller.

To better understand this tool, an example of the structure of the Controller's Record of Processing used directly by the TOD'S company is provided. Obviously, the real information for privacy compliance is not included, but concrete examples are provided to be able to better understand this document and the methodology employed by the company when compiling it.

Records of processing activities: Data controller section

Data Controller: *Company Name - Legal Office* (Via Filippo Della Valle 1, Sant'Elpidio a Mare (FM))

Representative of the Data Controller (where applicable):

Data Protection Officer (where applicable): *Privacy Ref. identifiers - Contacts (email, phone, etc.) (Alessandro Reni - dataprivacyofficer@todsgroup.com)*

ID	Cod. 002
Co-owners	Business name co-owners
Processing	Title of the treatment/process (e.g., Managing personnel recruiting process)
Description of the processing	Process description (e.g., receipt of CVs, interviews, etc.).
Notes	
Purpose	Indicate the objectives of processing activities (e.g., staff recruitment)
Description of purpose	
Legal Basis	Indicate the basis of lawfulness of processing (Art. 6.1 lett-(a) - (f) GDPR)
Complementary legal bases	Indicate whether there are other bases for lawful processing
Data Retention	Indicate the retention time for each purpose (e.g. 7 years)
Personal data categories	- Indicate the category of personal data processed (e.g. Common data (a) master data, (b) contact information; (c) economic information, etc. ; data belonging to special

	categories (a) data pertaining to health, (b) data pertaining to religious beliefs, etc.).
Data subjects	- Indicate type of stakeholders (e.g., customers, workers, etc.).
Data Processors	Provide company name, office, and contact information of suppliers who process personal data on our behalf.
Communication to third parties	Indicate whether data are transmitted to third parties who will act as autonomous data controllers (e.g., public administration, airlines in the case of worker travel, etc.).
Diffusion	Indicate if the data will be released into the public domain.
Extra EU transfer*	Indicate whether the data will be subject to extra-EU transfer, if so indicate country of destination and instrument of transfer (adequacy decision, Standard Contractual Clauses, BCR, etc.), and whether the data will be subject to transfer outside the EU. [Chapter V GDPR]
Treatment Modes. (Electronic, Non-Electronic, Both)	Indicate whether the data will be processed in paper and/or electronic form
Applications	- Indicate the information systems on which the data will be processed (e.g., SAP)
Paper archives	- Indicate the paper files in which the data will be stored (e.g., HR file)
Security measures	- Indicate the technical (e.g., data encryption), physical (security doors) or organizational (procedure for the proper use of company tools) security measures taken to protect the data processed in the process in question.

When one goes to fill out the record and define the treatments, an initial risk analysis is also carried out since among the various points there is also a general description of the technical and organizational security measures adopted by the company for a given activity. Thus, it is possible to understand the level of security at the beginning, without the adoption of the security measures, and the final one that consequently includes the protective measures. If even as a result of the protective measures, the risk is high (imminent risk), other security measures need to be taken and a DPIA (data protection impact assessment) needs to be completed.

The DPIA is essentially carried out when there is a technological innovation and a great risk to data subjects. TOD'S is a retail company and it is uncommon that they have to perform such assessments since the risks are never high and no particularly sensitive data is processed. The only case where a DPIA has been performed is in the large-scale video surveillance sector given its importance for the protection of personal data.

The DPIA is a somewhat more complex privacy risk assesment; it is always a good practice to do a privacy risk assesment before starting a process. However, GDPR introduced the principles of privacy by design and default, and if one complies with these principles, it is sort of like doing a privacy risk assesment in advance. For this reason, for many, DPIA is a measure in abundance and unnecessary. In Italy there is no standard structure for completing a DPIA. The situation is different in France where the French Data Protection Authority, the CNIL (Commission nationale de

l'informatique et des libertés), has its own online form that can be downloaded and in an easy and immediate way filled out.

5.6 IS THE GDPR STILL RELEVANT TODAY?

Thanks to the discussion with TOD'S DPO Alessandro Reni, it was possible to try to understand how current and up-to-date the GDPR still is and whether it is still powerful enough to protect citizens from emerging technologies. Through his work as a data protection officer he works closely every day with EU Regulations and data protection in general and constantly follows updates on the topic.

What follows is based on Mr. Reni's personal opinion and the discussion we had together.

The GDPR as soon as it came into effect was a really good tool. In terms of logic and form it was spot on, there had been a need for such an instrument for years that would put all companies, bodies and institutions on the same level and under the same rules. The information sector was growing enormously, and personal data was considered the new oil of the 21st century. Although it was a rather complex regulation, the necessary tools and information were being given to help those affected to comply with the regulation so that it was more understandable and implementable. The GDPR in 2018 was one of the most powerful personal data regulations in the world and provided the worldwide standard with the most stringent measures: if you complied with the GDPR you tended to be able to be

comfortable in whatever country you went to. It was a pathfinder for many states: think, for example, of the Californian Consumer Privacy Act (CCPA) in California, the Protection of Personal Information Act (POPI Act) in South Africa, and the Lei Geral de Proteção de Dados (LGPD) in Brazil. These are just a few examples of legislations that have taken the GDPR as a benchmark.

Four years after its implementation, it is still considered a very powerful policy tool, but more and more states are reaching the same level of protection and starting to legislate on areas where the GDPR may remain more lax. As a result, when European companies have to deal with legislation in non-EU countries, it will not necessarily be enough to comply with the principles imposed by the European Regulation in order to operate on foreign territory.

What is becoming more and more noticeable in recent years and is beginning to be a problem for all those who come into contact with EU rules is that the GDPR and the actions taken subsequently are moving somewhat away from the common feeling of citizens. The authorities, the guarantors have made some really on-the-nose choices that go to legislate on bureaucratic quibbles that take the simple and clear principles created initially to be very correct principles that often stray too far from the real world and common sense. Instead of protecting citizens, the views of guarantors often become triggered by political mechanisms that are pre-eminent over privacy. One example is all the antitrust sanctions they gave Google, or when they started accusing Google Analytics of exporting personal data, a similar thing

Facebook was accused of exporting data to the United States. But how can anyone accuse Facebook of exporting data when everything on social media is accessible by anyone? Or Google that like any cloud service exports data? The risk is that a European political vision mechanism is being triggered that wants to catch up with the big players in the US and China in terms of technology, and therefore GDPR is often used as a Trojan horse to achieve goals that go even beyond protecting the rights of European citizens. This does not create added value for the citizen and creates several problems for companies without increasing the level of personal data protection. Over time, there is a risk that instead of having a few clear, ironclad principles to respect that truly protect the European Union, a thousand technicalities that at the tip of the law risk fraying both the social and corporate fabric, and we end up respecting only what is convenient. Excessive bureaucracy creates more problems than benefits and risks making all legislation incomprehensible in the eyes of those involved.

If this mechanism were avoided, the GDPR would still be a very effective and current Regulation. The principles on which it is based and the responsibilities it has assigned to certain figures allow it to overcome any future obstacles brought by new technologies. Of course, special legislation will be needed to figure out how to regulate new digital tools such as artificial intelligence or the metaverse, but the foundations on which data protection is based are already laid and solid.

CONCLUSION

The protection of personal data is an issue that has become increasingly central to the legal landscape in recent years, reverberating its reflections also on economic, social and political scenarios around the world.

Often this topic is improperly defined by the broader concept of privacy, which represents an individual's personal space that strangers cannot trespass *("right to be left alone"*). The many evolutions of this right have created fertile ground for the development of a discipline that is as unique, certain and transparent as possible, aimed at the protection of the community territory. Over the years, it has led to talk of the right to the protection of personal data, which protects the individual's data, defined as that body of information relating to various aspects of a person's life (both private and social spheres), which the individual decides to make available to the "public" or, on the contrary, decides not to disseminate.

Europe is investing significantly on this right in the long-term perspective of shaping the future digital Europe that would be firmly grounded on common values and principles focused on the well-being of its citizens. The European Union itself, being aware of the repeated data breaches that have occurred throughout the years, understood that it was necessary to review the legislation and promulgate a new regulatory framework capable of ensuring better management of personal data in both small and medium-sized companies and large multinational corporations.

It is essential that all member states have common rules on which to base their activities, which is why it was decided to adopt a Regulation on the personal data protection. Unlike the directive, decisions, recommendations or opinions, the regulation is in fact a legal act of general scope that is mandatory in all its parts and directly applicable in the internal systems of the member states.

EU Regulation No. 679 of 2016, better known as GDPR, was created to achieve objectives of legal guarantee, administrative simplification and protection in the processing and transfer of personal data both within the European territory and outside the EU borders. In its current form, the Regulation can be seen as a necessary response to meet the future challenges that technological innovation poses to businesses; efficient data processing is a key element in ensuring economic growth. The GDPR introduces clearer provisions regarding the processing of personal data performed by the responsible figures (data controllers and data processors), while also defining the limits that companies place in order to ensure such processing. The legislation, in fact, establishes strict criteria that must be met when transferring data outside the European Union as well as specific and heavy sanctions if violations of the rules occur.

Commendable is the sharp change in perspective of the entire discipline now marked in maximum concentration on the prevention of harm and injury to fundamental rights that might result from a breach of security measures or unlawful treatment. This preventive-precautionary approach of the new system of protection

is explicitly captured in the establishment of particular institutes such as the pre-impact assessment, prior consultation with the supervisory authority, or even through the introduction of the principles of protection by design and by default thanks to which it is possible to elaborate all the necessary measures for data protection even before the processing is put in place and, at the same time, to ensure that only the personal data necessary for each specific purpose of the processing are treated.

Fundamental is the figure of the data protection officer for large companies, a specialized figure endowed with the character of professionalism and autonomy whose task is to assist the data controller while carrying out its tasks, but who at the same time turns out to be a point of reference and liaison both for the national guarantor authorities and for the data subjects themselves.

Therefore, GDPR compliance should not be considered as mere bureaucratic fulfilment since the adaptation of companies to this legislation qualifies as a key investment for the future in order to be able to meet the challenges of the market and emerging technologies.

In conclusion, in light of what has been said, it can be stated that the Regulation also has an important social function. Indeed, it seeks to promote in citizens and civil society a genuine culture of personal data protection. Given the fact that modern society is increasingly digitized, handling an increasing amount of data and the importance of whose confidentiality is increasingly emphasized, this shift can

only be positive in different directions and perspectives. As long as the legislation does not deviate from the common feeling of citizens and all measures are aimed at protecting personal data and adding value without getting stuck in bureaucratic quibbles, then Europe can be assured that it is walking on the right path and will be ready for whatever challenges come its way.

BIBLIOGRAPHY:

Allcott, H., & Gentzkow, M. (2/2017). *Social Media and Fake News in the 2016 Election.* Journal of Economic Perspectives.

Astone, M. (1/2020). *Right to be forgotten online e il discutibile ruolo dei gestori dei motori di ricerca.* Diritto di Internet, Digital Copyright e Data Protection.

Atomico. (2019). The State of European Tech. p. 215-216.

Boehm. (2012). Information sharing and data protection in the Area of Freedom, Security and Justice. Berlin: Springer.

Bonfanti, A. (3/2018). *Big data e polizia predittiva: riflessioni in tema di protezione del diritto alla privacy e dei dati personali.* Media Laws.

Commission, E. (February 2020). *Shaping Europe's digital future.* Luxembourg.

Craig, P. (2018). *EU Administrative Law, Third Edition.* Oxford University Press.

Donati, F. (2010). *Article 8−Protection of Personal Data, in Human Rights in Europe. Commentary on the Charter of Fundamental Rights of the European Union.* North Carolina: Carolina Academic Press.

Espas. (April 2021,). Global Trends to 2030: Challenges and Choices for Europe,. p.28.

Giovannini, E. (1/2016). La rivoluzione dei big data a sostegno dell'Agenda 2030. *Equilibri, Rivista per lo sviluppo sostenibile*.

Gonzalez, F. (2014). *The Emergence of Personal Data Protection as a Fundamental Right of the EU.* Springer.

Guehama, F. (January 2017). *Digital sovereignty - Steps towards a new system of internet governance.* Fondapol.

Heil. (2010). Directive 95/46/EC of the European Parliament and of the Council: Introductory remarks. Kluwer Law International.

Hijmans, H. (2016). *The European Union as Guardian of Internet Privacy.* Springer.

Jones, M. L. (2016). Ctrl+Z: The Right to be Forgotten. New York: New York University Press,.

Kirby, M. (1980). International guidelines to protect privacy in transborder data flows. *Jubilee conference*, (pp. p. 4, 14). Adelaide.

Kokott, J., & Sobotta, C. (4/2013). *The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR.* International Data Privacy Law vol. 3.

Kranenborg, H. (2008). *Access to documents and data protection in the European Union: On the public nature of personal data.* Common Market Law Review.

Krzysztofek, M. (2017). *Post-Reform Personal Data Protection in the European Union: General Data Protection Regulation (EU) 2016/679.* Kluwer Law International.

Kulk, S. (2015). *Freedom of Expression and "Right to be Forgotten" Cases in the Netherlands after Google Spain.* European Data Protection Law Review.

Lynskey, O. (2017). *The Europeanisation of data protection law.* Cambridge Yearbook of European Legal Studies.

Maat, A. B. (October 2019). *The EU's Regulatory Approach to Cybersecurity.* SWP.

MacCormick, N. (1999). *Questioning sovereignty: Law, State, and Nation in the European Commonwealth.* Oxford : Oxford University Press.

Martinez, D. F. (1/2018). *Unification of personal data protection in the European Union: Challenges and implications.* El profesional de la información.

Michael, J. (1994). Privacy and Human Rights: An International and Comparative Study, with Special Reference to Developments in Information Technology. Aldershot,: Dartmouth/UNESCO.

Pennisi, M. (n.d.). Così Bruxelles sta obbligando i colossi della tecnologia a occuparsi (seriamente) della privacy. *Corriere della Sera*, 10 luglio 2017.

Pernice, I. (5/2002). *Multilevel constitutionalism in the European Union.* European law review.

Piris, J. C. (2010). *The Lisbon Treaty: A Legal and Political Analysis.* Cambridge: Cambridge University Press.

Rasmussen, M., & Martinsen, D. S. (3/2020). *EU constitutionalisation revisited: Redressing a central assumption in European studies.* European Law Journal.

Renda, A. (2/2020). *Single Market 2.0: the European Union as a Platform.* College of Europe.

Rodotà, S. (2005). *Intervista su Privacy e Libertà a cura di Paolo Conti.* Roma: Editori Laterza.

Solinas, C. (2019). *La nuova figura del responsabile della protezione dei dati, in I dati personali nel diritto europeo.* Torino: Giappichelli.

Tzanou, M. (2013,). *Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right.* International Data Privacy Law.

Warren , S., & Brandeis, L. (1890). *The Right to Privacy.* Harvard Law Review.

SITOGRAPHY:

https://ec.europa.eu

https://www.mckinsey.com

https://www.cybersecurity360.it

https://www.inside.agency.com

https://gdpr-info.eu

https://www.ibm.com

https://www2.deloitte.com

https://www.onetrust.com/

https://clusit.it/

https://ico.org.uk

https://www.fendahl.com/

https://www.techtarget.com

https://www.consilium.europa.eu

https://ec.europa.eu/eurostat

https://privacycontrol.it/

https://www.bcg.com

https://home.kpmg

https://www.bain.com

https://www.tods.com

https://www.todsgroup.com