INSTITUTO DE ESTUDIOS
INTERNACIONALES
UNIVERSIDAD DE CHILE

# GDPR and Privacy Policies:

## The case of video games companies and data protection regulations.

# El GDPR y las políticas de privacidad:

## El caso de las compañías de videojuegos y las leyes de protección de datos.

Case study submitted in fulfillment of the requirements for the degree of Master in International Strategy and Trade Policy.

**Author: Camilo Agustín González López**

Supervisor: Prof. Fabiola Wüst Zibetti

September 24th, 2020

**Abstract**

This study sets out to identify the effects of the European Union's General Data Protection Directive (GDPR) on the videogames industry with regards to the policies of video game companies by analysing the changes made to the privacy policies of five video game companies during the last five years. In order to achieve this objective, the videogames industry, its users, and their personal data are characterized in the first chapter. The second chapter goes over the development of data protection regulations in the European Union, with special emphasis in the evolution of these regulations and the laws that came into force in 2018 with the GDPR. Finally, the third chapter analyses changes made to the privacy policies of five video game companies ((Valve Corporation, Nintendo, Electronic Arts, Take-Two Interactive y Ubisoft)) during the last five years in relation to the changes in regulation in Europe. This analysis shows that the new data protection standards have produced significant changes, as users now have clearly defined rights, companies are more transparent about data processing, and consent plays a more important part of the process than it did under the previous framework.

Key words: consumer rights, data protection, European Union, GDPR, personal data, video games.

**Resumen**

Este estudio tiene como objetivo identificar los efectos de la Regulación General de Protección de Datos (GDPR por sus siglas en inglés) en la industria de los videojuegos con respecto a las políticas de las empresas de videojuegos a través del análisis a los cambios hechos en las políticas de privacidad de cinco compañías en los últimos cinco años. Con el fin de cumplir este objetivo, el primer capítulo caracteriza la industria de videojuegos, sus usuarios y, especialmente, los datos personales de estos últimos. El segundo capítulo repasa el desarrollo de las políticas de protección de datos en la Unión Europea, con especial atención a la evolución de estas normativas y las reglas que entraron en vigor el 2018 con el GDPR. Finalmente, el tercer capítulo analiza los cambios en las políticas de privacidad de cinco compañías de videojuegos (Valve Corporation, Nintendo, Electronic Arts, Take-Two Interactive y Ubisoft) durante los últimos cinco años en relación a los cambios normativos en Europa. Este análisis muestra que los

nuevos estándares de protección de datos han promovido cambios en las políticas de protección de datos de la industria de videojuegos, haciendo que los derechos de los usuarios hayan mejorado, ya que los usuarios cuentan actualmente con derechos claramente definidos, las compañías son más transparentes respecto al procesamiento de datos y el consentimiento juega un rol mucho más importante para esta industria.

Palabras clave: datos personales, derechos del consumidor, GDPR, protección de datos, Unión Europea, videojuegos.

## TABLES AND GRAPHS.

# INTRODUCTION.

The protection of privacy and personal data is one of the main challenges of the digital era, as society is increasingly more dependent on new technologies such as machine learning and artificial intelligence. These technologies, as any other tool available to mankind, could have very negative or very positive consequences based on the uses we give to them. In this context, personal data has become a resource for various industries, especially the advertising industry and social media companies, who collect and trade people's personal data in order to improve their services and, by extension, increase their profits. Consequently, data protection laws are extremely necessary to prevent malpractices and abuses from both private companies and governments, with the latest development being the implementation of the European Union's General Data Protection Regulation, established in 2018.

The main objective of this study is to determine the effects of the General Data Protection Regulation on the video games industry, more specifically, on the data protection policies of video game companies. The first chapter of this study is divided into three sections: section 1.1 deals with the description of the global video games industry and its relevance based on financial and demographic variables obtained from different reports by the Interactive Software Federation of Europe and market research firms.; in section 1.2 videogame users and their personal data are described and characterized based on market research reports and case studies; and section 1.3 details the different uses of personal data by video game companies.

The development of data protection laws and regulations in the European Union is described in the second chapter, paying special attention to the changes between each document, in order to compare and contrast them based on the works of Julia Fromholz, Francoise Gilbert,

Burri Mina and Rahel Schär, among others. The first section of this chapter studies the first data protection regulations in Europe and the world from national laws in countries such as Germany and France up until the creation of the GDPR in 2016. The second section goes into detail about the GDPR's preceding regulations: the Council of Europe's (COE) "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data from 1981" and the "Data Protection Directive" of 1995. The third section of this chapter outlines the main features of the GDPR, paying special attention to the changes introduced by this regulation.

In the third chapter, the application of the changes brought by the GDPR is analysed through a qualitative analysis of the privacy policies of five video game companies: Valve Corporation, Nintendo, Electronic Arts, Take-Two Interactive, and Ubisoft. These five companies were selected based on brand recognition and revenue for the last quarter of 2019. The focus of this chapter is in the changes made to the privacy policies of these five companies in the last five years, period on which the GDPR was created and passed as a law, which can be seen by comparing the current versions of these policies to their previous versions.

This case study is relevant to this Master's Degree from the perspective of international strategy, as international companies operating in Europe from all origins have had to adapt to the GDPR and the new data protection standards, which could even be replicated in other regions of the world. In this sense, the US-EU Privacy Shield is one example of data protection laws being a matter of trade policy for countries outside the European Union as foreign governments look to ensure the proper access to the European market for companies from their own countries. Additionally, countries like Chile are susceptible to be influenced by this type of policies as the EU has introduced elements such as the 'democracy clause' in some of their trade agreements.[1]

[1] https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU%282017%29558764

This could be considered as an opportunity for Chile to further develop its data protection laws and be at the forefront of the protection of personal data.

# CHAPTER 1: USER DATA IN THE VIDEO GAME INDUSTRY.

This first chapter aims to characterize video games, the industry surrounding them, and the types of personal data collected and processed by video game companies. This will be achieved by describing video games and their main characteristics, functions, and classifications. To better understand the video games industry, I will refer to market and industry reports to measure revenue, number of users and growth at a global and regional scale. Different examples will be used to outline the types of data being collected and why it is necessary to have higher data protection standards than the current ones in most of the world.

## 1.1. The Video Game Industry: the Global Market.

A video game is defined by the Cambridge Dictionary as "a game in which the player controls moving pictures on a screen by pressing buttons"[2], an extremely vague definition that illustrates the extensive nature of such a product. In similar straightforward fashion, Nicolas Esposito defined video games in 2005 as "a game which we play thanks to an audio visual apparatus and which can be based on a story," which differentiates itself from a regular game due to its audio visual apparatus or "electronic system with computing capabilities, input devices and output devices."[3][4] From a philosophical approach, Jonne Arjoranta argues that "there is no final definition of [computer] games as long as there are people capable of both playing games and thinking about them,"[5]which points to the fact that, as a medium for cultural expression, video games are ever-changing depending on both their cultural and technological context.

---

[2] *Cambridge Dictionary*, s.v. "Video Game," https://dictionary.cambridge.org/dictionary/english/video-game
[3] Esposito, Nicolas. 2005. *A Short and Simple Definition of What a Videogame Is*. Centre de recherches, Compiègne: University of Technology of Compiègne.
[4] Idem.
[5] Arjoranta, Jonne. "How to Define Games and Why We Need to." *The Computer Games Journal* (2019): 109-120.

Taking these precedents into consideration, we will understand video games as any kind of game that is played in a digital device for purposes such as entertainment, socializing, education, competition, and/or profit. This definition is broad enough to include all digital devices (i.e. mobile phones, personal computers, and video game consoles) while also being quite specific in the player's motivation to engage with a video game. The reason why video games can be played for many different purposes is that, most of the time, they are simulating a reality that has to, at least somewhat, resemble our own, thus making it open to the same motivations and objectives that a person can have outside a digital world.

One of the most recurrent examples is Blizzard Entertainment's *World of Warcraft*, a Massively Multiplayer Online Role Playing Game (MMORPG) based in a mediaevalesque fantasy universe, which provides players with an extensive story arc that amounts to a few hundred hours of playtime that is expanded every few years with the release of new expansions. In this world, players can enjoy the game's story, be a part of a guild and meet new people from all over the world, participate in massive boss battles with their friends or with random people, try to defeat the game's latest bosses in the shortest time possible in order to gain the community's recognition[6], learn about a variety of school related subjects with the guidance of their teachers[7], or simply gather resources to buy subscription tokens with-in-game currency and sell them for real money[8].

A more traditional classification of video games provided by the Interactive Software Federation of Europe (ISFE) focuses on the device in which the game is played and includes

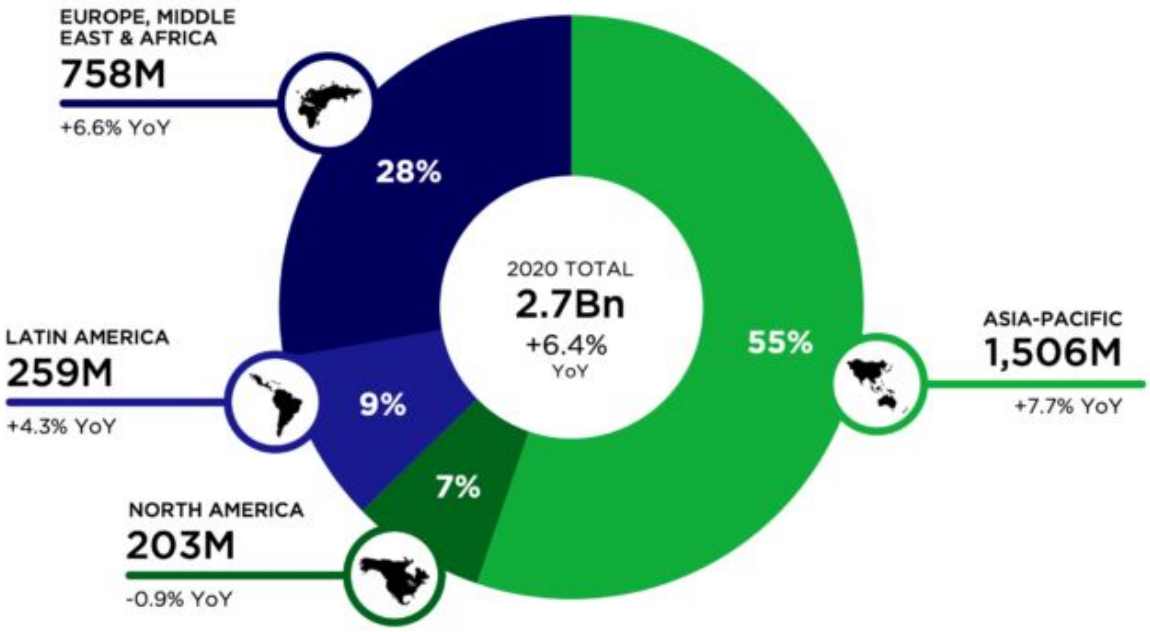
[6] "What Does It Cost to Be Crowned WoW World First Champions?" PCGamesN, accessed September 2, 2020, https://www.pcgamesn.com/world-of-warcraft/wow-world-first-complexity-limit
[7] "World of Warcraft in School," PB Works, accessed August 28, 2020, http://wowinschool.pbworks.com/w/page/5268731/FrontPage
[8] "The Rise of Gold Farming in China," Venture Beat, accessed August 28, 2020, https://venturebeat.com/2011/07/22/the-china-conundrum-the-rise-of-gold-farming/

home consoles such as the current PlayStation 4 by Sony, Xbox One by Microsoft, and Nintendo Switch by Nintendo; mobile phones, tablets and other smart devices; personal computers regardless of their operative system; and handheld devices the such as Sony's PlayStation Vita and Nintendo's 3DS. The reasons why an individual chooses one device over another vary wildly as these devices tailor to different preferences and socioeconomical contexts. According to ISFE's data, computers are the most common platform for video games with 56%, followed by video game consoles with 50%, smartphones with 48% and, tables with 27% and, lastly, handheld consoles with 17%.[9]

The global video games industry has a considerable presence in all markets and earned a total of USD $109.4 billion in 2019, comprising $64.4 billion from mobile games, $29.6 billion from computer games, and $15.4 billion from console games according to SuperData.[10] In terms of userbase, it is estimated that 2.7 billion people play video games in the world, with 1.5 million players in the Asia Pacific region, 758 million players in the Europe, Middle East and Africa region, 259 million players in Latin America, and 203 million players in North America, according to market research company Newzoo[11], which can be seen in figure 1.

[9] Interactive Software Federation of Europe. 2019. "Key Facts 2019." PDF.
[10] SuperData. 2020. 2019 Year in Review. PPT Presentation, SuperData
[11] Newzoo. 2020 Global Games Market Report. April, 2020. https://newzoo.com/key-numbers/

**Figure 1: Number of video game players by region for 2020.**



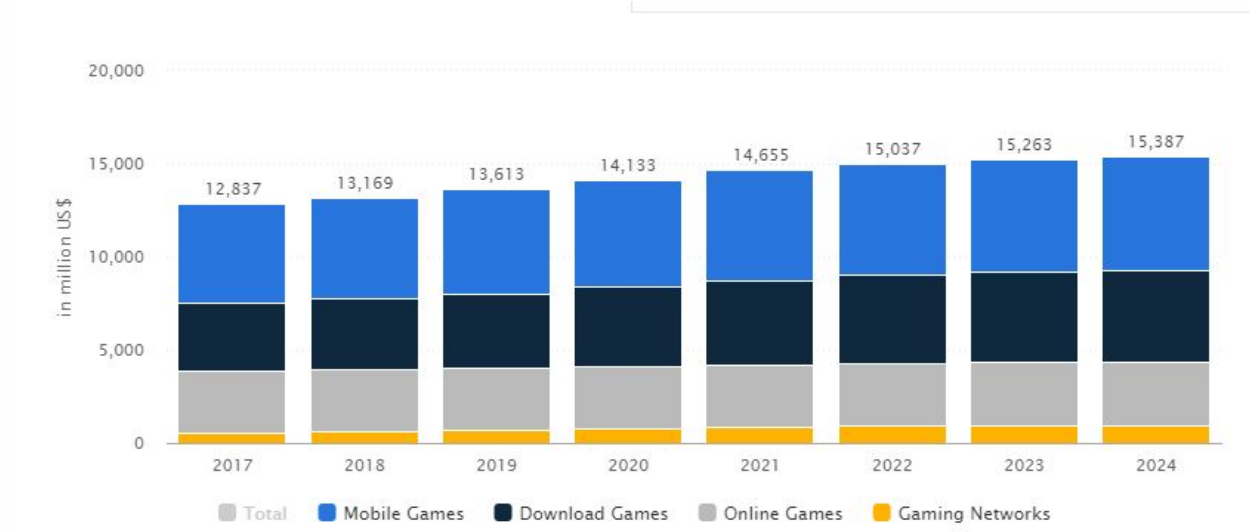

Source: Newzoo. 2020 Global Games Market Report. April, 2020. https://newzoo.com/key-numbers/

The ISFE provides its own data about the video games industry's revenue in Europe which, according to the its "Key Facts 2019" report, was around US$13.5 billion[12] for 2018. According to Statista, the video games industry in Europe reached a revenue of US$13,169 million in 2019 as seen in figure 2, with the mobile video games industry being the highest grossing platform at US$5,569 million. In comparison, the video games industry in the United States generated a revenue of US$18,425 million, while China's reached US$26,149 million,[13] making the European market the third biggest market in the world. The global video games

[12] According to the rates for January 2019 provided by exchangerates.org.uk https://www.exchangerates.org.uk/EUR-USD-spot-exchange-rates-history-2019.html
[13] According to the rates for January 2019 provided by exchangerates.org.uk https://www.exchangerates.org.uk/EUR-USD-spot-exchange-rates-history-2019.html

industry received a revenue of US$120.1b in 2019 according to Superdata.[14] Considering these numbers, it can be stated that the European video games industry accounts for 11% of the global video games industry, making it one of the most important markets for the industry.

**Figure 2: Video games industry revenue in Europe.**




Source: Video Games - Europe: Statista Market Forecast https://www.statista.com/outlook/203/102/video-games/europe

The video game industry's interests are represented mostly by the ISFE, which groups 17 international video game companies that operate in Europe and 12 national trade associations of developers and publishers from 15 countries. Its board is composed by executives from its member companies and trade associations, and its mission is defined as to ensure "that the voice of a responsible games ecosystem is heard and understood, that its creative and economic potential is supported and celebrated, and that players around the world continue to enjoy great video game playing experiences."[15] In other words, the ISFE's main purpose is to represent the

[14].SuperData, 2020.
[15] Interactive Software Federation of Europe. n.d. About ISFE. Accessed May 2020, 18. https://www.isfe.eu/about-ifse/

interests of its stakeholders by ensuring a suitable environment for economic and creative growth.

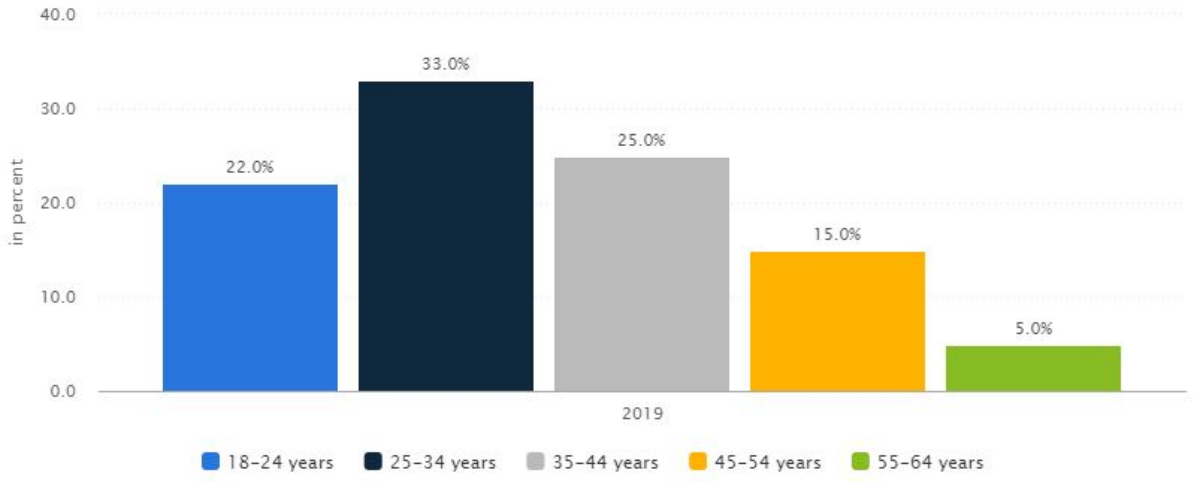
**1.2. The video game industry's users and their data.**

In terms of its userbase, the video games industry in Europe is reported to have around 278.3 million individual users, out of which 63% are male and 37% are female[16], as figure 3 illustrates. According to the ISFE, the gender gap is much smaller, as it reports that 46% of EU gamers are women while 54% are men.[17] Based on this, we can argue that even though a majority of video game players in Europe are men, the gender gap is not as big as one might be inclined to believe.

When classified by age[18], the biggest age group is the one between 25-34 years, accounting for 33% of the total userbase, followed by users between 35-44 years with 25% and between 18-24 years with 22%, meaning that 80% of European video game players are 54 years old or younger. The ISFE demographics for 2018 present the data in a different way, as it shows the percentage of people from a determined age group that play video games, as seen in figure 3. In this regard, the data shows that over 74% of people aged 6 to 24 play video games, with the 11-14 segment having the highest percentage at 84%. Older age groups still have relevant shares of gamers that decline as age increases, going from 67% for people aged 25-34 to 34% for people aged 45-64, with people aged 35-44 sitting in between with 49%. It should be noted that the ISFE's data considers only the markets of France, Germany, Spain and the United Kingdom.

[16] "Europe: Statista Market Forecast," *Statista.* Last accessed: May 18, 2020. https://www.statista.com/outlook/203/102/video-games/europe#market-users.
[17] Interactive Software Federation of Europe. 2019. "Key Facts 2019." PDF.
[18] " Europe: Statista Market Forecast"

**Figure 3: European video game players by age group.**




Source: Video Games - Europe: Statista Market Forecast https://www.statista.com/outlook/203/102/video-games/europe

The last relevant category in terms of userbase classification is the revenue from the four markets previously mentioned, which is divided into three categories: online revenue, app revenue and physical revenue, which represent 40%, 34% and 26% of the total revenue for 2018 according to the ISFE.[19] Considering these two categories it can be clearly seen that pc gaming is both the main platform and the main source of revenue for video games in Europe, closely followed by video game consoles and mobile gaming.

All of these statistics show a very simple yet relevant fact: most Europeans play video games. Regardless of platform, gender, and age, a majority of EU citizens are either casual or hardcore gamers and, as such, give their data to video game companies in different degrees. In this context, the information collected by video game companies can vary from the aforementioned demographics to behavioural data such as spending patterns, information that is not only valuable from a personal standpoint, but also highly valued from a commercial and marketing perspective, making their protection a priority.

[19] Interactive Software Federation of Europe. 2019. "Key Facts 2019." PDF.

The amount and types of personal data collected by video game companies vary depending on multiple conditions such as the device used, internet connection (or lack thereof), and type of game. In this sense, some video games may only request and store login data such as an email address, name, and date of birth, while others may store the player's credit card information, physical address, social media accounts, and behavioural patterns.

A 2018 study[20] published in the *Fordham Law Legal Studies Research Paper* analysed the types of data collected concluded, along with the usual information consciously provided by the player, "location data and biometric data - like facial, voice, heart rate, weight, skin response, brain activity, and eye-tracking data - is now routinely collected while gaming"[21] through hardware, social features, and tracking technologies, which allows companies to not only create a psychological profile for their users but also a physical profile. The collection of these types of data makes video game companies a target of cyber-attacks, as hackers try to gain access to a company's database in order to extract all their available user data, which can then be used to make fraudulent purchases or simply be sold to a third party, depending on the type of data obtained. [22][23]

Considering these precedents, the types of personal data have been divided into six different categories along with some examples, which are not comprehensive and can include other data. Additionally, it is important to remember that the value of personal data comes from

[20] Russell, N. Cameron, Joel R Reidenberg, and Sumyung Moon. 2018. Privacy in Gaming. New York: Center on Law and Information Policy.
[21] Russell, Reidenberg and Sumyung, 2018.
[22] Data Breach Warning for 200 Million iOS and Android gamers. Forbes. 2019. https://www.forbes.com/sites/daveywinder/2019/09/30/data-breach-warning-for-200-million-android-and-ios-gamers/#2ec990461db3
[23] EA Games Leaks Personal Data of 1600 FIFA 20 Competitors. Inforsecurity Magazine, 2019. https://www.infosecurity-magazine.com/news/ea-games-leaks-personal-data/

the possibility of merging different sources of information in order to understand or even predict a user's behaviour, usually with marketing purposes.

- **Identifiable data:** Names and last names, email addresses, home address, country of residence, telephone number, location.
- **Financial data:** credit card number, bank account information, billing address, purchase history.
- **Social data**: friends, social network profiles and posts, phone contacts.
- **Behavioural data**: time spent on certain activities, purchasing patterns, interests and preferences.
- **Technical data**: device, operative system, network used, IP addresses.
- **Biometric data**: facial features, voice, height, weight, fingerprints, heart rate.

As Charles Duhigg wrote in an article for *The New York Times Magazine*[24], most companies nowadays collect as much personal data as possible, using North American retail company Target as the main example. According to Duhigg, Target collects "demographic information like your age, whether you are married and have kids, which part of town you live in, how long it takes you to drive to the store, your estimated salary, whether you've moved recently, what credit cards you carry in your wallet and what Websites you visit,"[25] allowing Target to create a fairly accurate customer profile that makes it easier to target their marketing. If that profile is not complete enough there are plenty of available databases for sale, as Duhigg states that

[24] How Companies Learn Your Secrets. Charles Duhigg. The New York Times Magazine, 2012. https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=1&_r=1&hp
[25] Duhigg, 2012.

> Target can buy data about your ethnicity, job history, the magazines you read, if you've ever declared bankruptcy or got divorced, the year you bought (or lost) your house, where you went to college, what kinds of topics you talk about online, whether you prefer certain brands of coffee, paper towels, cereal or applesauce, your political leanings, reading habits, charitable giving and the number of cars you own.[26]

This makes it easier for companies like Target to understand their customers' habits and aim their ads in order to get customers to shop at Target instead of Walmart, for example. The use of these data sets can extend beyond targeted marketing, with the best example being China's social credit system that "aims to construct a database that monitors the behaviour of individuals, corporations and governmental entities across China in a contemporaneous manner."[27]

### 1.3 User data in the videogame industry

In terms of the uses that video game companies give to the data of their users, one of the main classifications is the internal and external use of data, i.e. if it is being shared with third parties and for what purposes. In this sense, companies may collect data in order to contact a user and to provide goods and services among other possible internal uses. Additionally, companies might share a user's personal data in order to deliver certain services such as customer service, technical assistance, and social features, among others. Some companies might even sell the user's data to other companies for purposes such as people search, credit reporting, advertising and marketing, and risk mitigation.[28]

Video game players' personal data is not only vulnerable to attacks by third parties but it can also be used to gather additional information from the player and create psychological

---

[26] Duhigg, 2012.
[27] An Introduction to China's Social Corporate Credit System. New Horizons, 2020. https://nhglobalpartners.com/chinas-social-credit-system-explained/
[28] Melendez, Steven and Alex Pasternack, "Here are the data brokers quietly buying and selling your personal information", Fast Company, 2019 https://www.fastcompany.com/90310803/here-are-the-data-brokers-quietly-buying-and-selling-your-personal-information

profiles by cross referencing the information provided by the player. Sam Barlow, writer of video game *Silent Hill: Shattered Memories* (2010) explains in an interview with website Polygon[29] the psychometric evaluation undertaken by players at the beginning of the game, which allows the game to change its story based on the players' answers by weighing psychological traits such as respect for authority figures in order to "subvert expectations and heighten drama"[30] as Barlow explains. Luckily for *Silent Hill* players, this information was only used for the story's sake, something that could have been very different if the game were to be released today instead of 2010.

The same Polygon article includes an interview with Josh Sawyer, design director at video game development company Obsidian Entertainment. In a similar fashion to *Silent Hill*, Obsidian's 2010 *Fallout: New Vegas* also included a personality test at the beginning of the game in order to allow players to customize their character's personality. The danger of such a feature, argues Sawyer, lies on the possibility of using this kind of data for other purposes such as predicting a player's future behaviour, especially because "there was no psychological rigor behind [the test]."[31] Even if some companies, such as Obsidian, offered players the option to not have their data collected, not all companies allowed players to refuse it.

Despite the fact that malpractices leading to class action lawsuits from users or fines by European authorities have not been detected in the video games industry, the personal data collected through video games is too sensitive to not be legally protected from companies such as Epic Games, which will be explained in the third chapter of this study. This means that even the slightest possibility of video game players' personal data being misused or stolen presents an

[29] "The Dangers of in-game Data Collection," *Polygon*. 2019. https://www.polygon.com/features/2019/5/9/18522937/video-game-privacy-player-data-collection
[30] "The Dangers of in-game Data Collection."
[31] "The Dangers of in-game Data Collection".

incredible risk that is not worth taking. In this sense, data protection regulation is not only recommended but necessary across all industries, something that the European Union has understood and led to the creation of different data protection regulations dating as far back as 1981, which will be analysed in the following chapter.

# CHAPTER 2: DATA PROTECTION IN THE EUROPEAN UNION.

This episode aims to describe and analyse the development and evolution of data protection standards in the European Union, by going back to its very beginning in the last decades of the XXth century, passing through the Data Protection Directive of 1995 and arriving at the current applicable law, the General Data Protection Regulation. Special attention will be placed on the changes from one regulation to the other and the context in which these changes were made in order to understand the intentions behind these changes and measure their relative success. The definitions for most of the technical terms used in these regulations can be found in the appendix of this study for further clarification.

## 2.1. The evolution of data protection regulation

Even though *data protection* is a fairly recent legal term, established in an international setting by the Council of Europe's (COE) "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data from 1981"[32] (*the convention*), its legal roots can be traced to the protection of privacy as early as the 19th century.

It was the work of Samuel D. Warren and Louis D. Brandeis, who in 1890 published their article "The Right to Privacy" in Harvard Law Review,[33] that gave privacy the spotlight it needed from a legal point of view. As technology advanced in the last century, new forms of data collection were developed, and so did privacy and later data protection laws. In this sense, Warren and Brandeis' article dealt mostly with the protection of privacy against tabloids and the use of still image cameras and it became one of the first legal works arguing the need to legally protect a person's right to privacy.

[32] Council of Europe. 1981. "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data." Treaty, Strasbourg. https://rm.coe.int/1680078b37

[33] Warren, Samuel D., and Louis D. Brandeis. 1890. "The Right to Privacy." Harvard Law Review 4 (5): 193-220. Accessed May 18, 2020. doi:10.2307/1321160.

In the international context, the "Universal Declaration of Human Rights" in 1948 by the United Nations and the "European Convention on Human Rights" (1950) by the COE established privacy as a human right, which would set a baseline for the protection of privacy from which States would build their own legislation. With the introduction of computers in the following decades the concept of privacy evolved to include the protection of personal data and the international community began to slowly incorporate this new concept into both national laws and international agreements. The COE's convention is the first international legal document to address the protection of personal data, preceded by the national legislation on the subject in countries such as Germany (1977)[34], France (1978)[35], Norway (1978)[36] and Denmark (1978)[37] and the OECD guidelines on data protection (1980)[38], with the latter outlining many of the principles that would be included in the convention.

The first article of the convention on personal data states its purpose as "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,"[39] establishing data protection as a legal obligation for the signing parties. As the first international treaty on the matter it only established general guidelines and obligations, and it did not concern itself with the volume of data being processed as the internet had not been developed yet.

---

[34] Gesetz zum Missbrauch personenbezogener Daten bei der Datenverarbeitung [Act Concerning the Abuse of Data in Data Processing], Jan. 27, 1977. https://dejure.org/BGBl/1977/BGBl._I_S._201

[35] Loi Informatique et Libertes [Act on Information Technology, Data Files and Civil Liberties], Jan 6, 1978. https://www.cnil.fr/sites/default/files/typo/document/Act78-17VA.pdf

[36] Personvernlovgivningen er 40 år [La ley de datos personales tiene 40 años], Knut Kaspersen, June 8, 2018. https://www.personvernbloggen.no/2018/06/08/personvernlovgivningen-er-40-ar/

[37] The Right to Privacy in Denmark, Privacy International and IT-Political Association of Denmark, June 2015. https://privacyinternational.org/sites/default/files/2017-12/Denmark_PI_UPR%20Stakeholder_submission_FINAL.pdf

[38] Thirty years after the OECD privacy guidelines, OECD, 2011. http://www.oecd.org/sti/ieconomy/49710223.pdf

[39] Council of Europe. 1981. "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data." Treaty, Strasbourg. https://rm.coe.int/1680078b37

In fact, as Julia M. Fromholz (2000) indicates, "the council has largely failed to achieve uniform protection for personal data (…) because it could not force countries to implement its Convention through legislation,"[40] making the ratification of the treaty a rather symbolic act. Nevertheless, the convention still marked an important milestone in data protection as five European countries ratified it by the date it entered into force in October 1985 and 55 countries have signed and ratified it as of 2019, including 8 non-European countries.

The next legal document from the European Union relating to data protection was the Data Protection Directive of 1995 (Directive 95/46/EC, *the directive*)[41], which aimed to provide a common framework for the member states to develop their own data protection laws without imposing a specific legislation, understanding the different levels of technological development at that time and the different needs of each country. The directive led to the Commission decision of 2000[42] "pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce", which established several principles of data protection for US companies, in order to store and process data from EU citizens in the United States.

The directive was complemented with the Data Retention Directive of 2006 (Directive 24/EC), which regulated the retention of personal data for purposes of law enforcement. This directive was later derogated by the EUCOJ in 2015 as it considered that it violated the

[40] Fromholz, Julia M. "The European Union Data Privacy Directive." Berkeley Technology Law Journal 15 (1) (2000): 461-484

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

[42] "Commission Decision of 26 July 2000," *Official Journal of the European Communities* (2000): https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ%3AL%3A2000%3A215%3A0007%3A0047%3AEN%3APDF#:~:text=Done%20at%20Brussels%2C%2026%20July%202000.&text=The%20European%20Union%27s%20comprehensive%20privacy,adequate%27%20level%20of%20privacy%20protection.

fundamental rights of European citizens by allowing governments to access traffic and location data collected by private companies which had to be stored for a period of up to two years. That same year, the same court declared the Safe Harbour Agreement invalid as it did not guarantee a minimum level of data protection with regards to the fundamental rights of EU citizens. These cases were two of the main reasons for the creation of the current General Data Protection Regulation in 2016, which not only meant to standardize data protection laws across the continent but also to provide higher levels of protection for its citizens.

**2.2. Data protection before GDPR.**

The European Union's Data Protection Directive was adopted in 1995 as the first piece of legislation on the subject by the EU. In a similar fashion to the convention, its first article defined its objective as to "protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data,"[43] which would be met by providing minimum standards for data protection throughout the EU that its members can then turn into legislation.

The broader scope of the directive, compared to the convention, can be noticed immediately in their definitions, as the convention only defines *personal data*, *data subject*, *automated data file*, *automatic processing*, and *controller of the file*,[44] while the directive defines *personal data*, *data subject*, *processing (of personal data)*, *(personal data) filing system*, *controller*, *processor*, *third party*, *recipient*, and *the data subject's consent*, [45] illustrating the

[43] European Union. 1995. "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data." Directive.
[44] Council of Europe. 1981.
[45] European Union. 1995.

evolution and increasing complexity of technology and data usage ( for their legal definitions refer to appendix). Some of the common features of both documents are the obligation from data processors to handle data fairly and lawfully, to collect it only for specified and legitimate purposes agreed upon by the data subject, and the obligation from governments to ensure that personal data may only be processed under certain conditions, such as when absolutely necessary and after the data subject has agreed to have his data processed.

On the one hand, the convention did not intend to override the national law of the signatory parties but to provide basic standards of data protection as it established special categories of data, which could not be processed automatically such as religious beliefs, political opinions and racial origin[46], while setting minimum standards for the automatic processing of data detailed in Article 5. Along with that, the convention also required the parties to establish a specific authority to coordinate communication between them and allow their citizens to exercise their legal rights when residing in the territory of another party, being this one of the most significant articles in terms of practical changes introduced.

The directive, on the other hand, can be divided into five main topics, according to Francoise Gilbert[47], while still maintaining most of the convention's key features: **confidentiality and security of the data**, **rights of the data subject**, **direct marketing**, **compliance requirements**, and **transfers outside the European Economic Area**.[48]

In terms of **confidentiality and security of the data**, it establishes minimum standards for the data's controller and processor when handling personal data, ranging from ensuring the

[46] Council of Europe, 1981.
[47] Gilbert, Francoise. 2007. "A Bird's-Eye View of Data Protection in Europe." GPSolo (American Bar Association) 32-35
[48] Gilbert, Francoise. 2007. "A Bird's-Eye View of Data Protection in Europe." GPSolo (American Bar Association) 32-35

security and confidentiality of the data to the monitoring of subcontracted processors to ensure that the data is being protected.[49]

**Rights of the data subject** refer to the different tools to control their information given to data subjects in this document, including the right to know the type of data that is being collected, when, for what purpose and by whom, along with the right to have their data deleted, the ability to challenge decisions concerning themselves based on this same data and the right to refuse direct marketing based on their personal data. Similarly, the section related **direct marketing** makes the data subject's consent a prerequisite in order to use his personal data for marketing. In order to ensure that the **compliance requirements** are met, the directive required the creation of a national supervisory authority that would monitor data controllers and processors.[50] Finally, regarding **transfers outside the European Economic Area**, the directive established the need for non-members of the EEA to guarantee an adequate level of protection before being able to receive and process data from an EEA data subject.[51]

The shortcomings of the directive and the need to modernize data protection laws were highlighted by three key issues that resulted in three court rulings that made the need for a new data protection regulation evident .[52] The first key issue was the '**right to be forgotten**' (brought up by the *Google Spain* case[53]), which, exactly as its name indicates, refers to an individual's right to have their personal data removed from indexes and search engines if that information is

[49] Gilbert, Francoise. 2007. "A Bird's-Eye View of Data Protection in Europe." GPSolo (American Bar Association) 32-35
[50] Gilbert, Francoise. 2007. "A Bird's-Eye View of Data Protection in Europe." GPSolo (American Bar Association) 32-35
[51] Gilbert, Francoise. 2007. "A Bird's-Eye View of Data Protection in Europe." GPSolo (American Bar Association) 32-35
[52] Mina, Burri, and Rahel Schär. "The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy." Journal of Information Policy (Penn State University Press) 6 (2016): 479-511.
[53] "Judgment of the Court (Grand Chamber)" *EUR-Lex* (13 May 2014): https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131

not of public interest. This case was resolved in favour of the plaintiff by determining that data subjects have the right to request the deletion of links to websites containing data about them from indexation and search engines such as Google.[54]

The second relevant issue was the **storage of personal data by service providers for longer than necessary**, so that national governments could access this data. This issue was discussed in the case Digital Rights Ireland against the EU[55] over the Data Retention Directive 2006/24/EC, which allowed said storage of personal data for national governments, intelligence agencies and police bodies to access and was one of the antiterrorist measures taken by the EU after the terrorist attacks of the early 2000s. The fact that this directive allowed governments to access the personal data of all their citizens without probable cause meant that, according to the COJEU, it went against the EU's Convention of Human Rights in its articles 7 and 8 which establish respect for privacy and the right to the protection of personal data.[56] Even though the court decided to invalidate directive 2006/24/EC, this case highlighted the need to protect personal data not only from private companies but also from national governments, something that the 1995 directive did not guarantee.[57]

The third main issue with the data protection regulations before 2016 was related to **international data transfers**, which was discussed in the case of Maximillian Schrems against the Irish Data Protection Commissioner (the Commissioner) over the Commissioner's dismissal of Schrems' complaint against Facebook Ireland.[58] In his complaint, Schrems argued that "by transferring user data to the United States, Facebook Ireland was facilitating the processing of

[54] Mina and Schär (2016).
[55] "Judgment of the Court (Grand Chamber)" *EUR-Lex* (8 April 2014): https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293
[56] "Charter of the Fundamental Rights of the European Union" *Official Journal of the European Union* (26 October 2012): https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:12012P/TXT
[57] Mina and Schär (2016).
[58] Schrems vs Data Protection Commissioner (2014) http://www.bailii.org/ie/cases/IEHC/2014/H310.html

such data by Facebook itself"[59] in the United States, which would leave European citizens' personal data unprotected by the EU's own standards given the lack of data protection regulations in the US. This was dismissed by the Commissioner under the 'Safe Harbour'[60] agreement between the EU and the US ratified by the Commission of the European Communities, under which American companies could self-certify themselves as compliant with seven data protection principles.

The importance of this case, in the same vein as the other two, lies on the conclusions by the High Court of Ireland, as it establishes that even if the Commissioner was right in its actions based on the 1995 Directive and the 2000 Commission Decision, these agreements did no longer hold up given the political and technological developments of the last 20 years. This was followed by the 2015[61] decision by the COJEU establishing that supervisory authorities must investigate all complaints regarding the transfer of personal data to third countries, especially in terms of their compliance to the 1995 directive. In other words, this ruling invalidated the Commissions' decision and the Safe Harbour agreement, reinforcing the fact that data protection laws needed to be updated with urgency, which ultimately led to the creation of the EU's General Data Protection Regulation.

After the legal and normative flaws of the directive and the following regulations built upon it were made evident by these three cases, it was announced in 2015 by the European Council that a new data protection regulation would be developed and implemented after three

[59] Schrems vs Data Protection Commissioner. 2014.
[60] "Commission Decision" *EUR-Lex* (26 July 2000): https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32000D0520
[61] Court of Justice of the European Union. "The Court of Justice declares that the Commission's US Safe Harbour Decision is." Press Release, Luxemburg (2015): https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdfe

years of discussion,[62] which resulted in the creation of the General Data Protection Regulation of 2016.

### 2.3. Data Protection after GDPR.

Adopted in April 2016 and implemented in May 2018, the General Data Protection Regulation can be seen as the EU's strongest effort to date in terms of data protection. According to Mina and Schär, the first notable difference between the GDPR and the 1995 Directive is indicated by their names, as in the EU's legal system a Directive "defines the results to be achieved leaving the choice of the means for achieving them up to the Member States"[63] while a Regulation "is directly applicable and does not require additional domestic implementation." This means that, even if their contents are the same, the GDPR will be much more effective in its implementation than the Directive, a measure that can at least assure the harmonization of data protection laws within the EU. These same authors classify the main changes brought by the GDPR in three categories: **stronger consumer rights**, **more obligations for data controllers and processors**, and **territorial scope of application**,[64] same categories that will be used here to explain these changes.

In terms of **consumer rights**, chapter III of the GDPR is named **Rights of the Data Subjects** and, as the name indicates, outlines not only said rights but also the modalities for their exercise as well as the timeframes the data subjects' requests and communication channels that should be available for these requests. [65] Article 13 and 14 of the same chapter list the

[62] Data Protection: Council Agrees on a General Approach. Council of the EU, June 15, 2015. Council of the EU. https://www.consilium.europa.eu/en/press/press-releases/2015/06/15/jha-data-protection/
[63] Mina and Schär (2016).
[64] Mina and Schär (2016).
[65] Article 12, GDPR.

information that should be provided by the data controller to the data subject both when personal data is collected from the data subject and when it is obtained from a third party, including contact information for both the controller and the data protection officer, the purposes for which the data is being collected, and third party recipients of their personal data. These provisions are directly linked to the **right of access by the data subject**, which is explained in Article 15, that lists in more detail the information that should be available to data subjects.

Article 16 and 17 refer to the right to rectification and the right to erasure (also known as the **right to be forgotten**), which allows data subjects to correct any inaccurate personal data a controller may have and to have their data erased under certain conditions. Some of the conditions for data erasure include withdrawal of consent from the data subject, unlawful processing of personal data, and the personal data no longer being necessary for the purposes for which it was collected. Article 18 established the **right to restriction of processing**, which allows the data subject to have their data restricted, e.g. it can only be stored without the data subject's consent, when its accuracy has been contested, when its processing is unlawful, when it is no longer necessary for the purposes of processing, and when its processing has been objected by the data subject.

Article 20 explains the **right to data portability**, which is meant to ensure that when a data subject obtains their data from a controller it is "in a structured, commonly used and machine readable format"[66] in order to have their data processed by another controller. Article 21 deals with the **data subject's right to object**, which means that the subject can object to the processing of their data at any point during the processing process. Controllers can appeal this right if they can demonstrate "compelling legitimate grounds" for the processing of the data that

[66] Article 20, GDPR.

are above the subjects interests, rights and freedoms.[67] Data subjects can also object to having their data processed for direct marketing and for historical or scientific purposes, with the latter not being able to be objected to if it is being processed for reasons of public interest. Finally, article 22 states that "the data subject shall have the right not to be subject to a decision based solely on automated processing" if it has legal ramifications or has a similar impact on their life.

The increasing obligations for data controllers and processors are outlined in chapter IV, named **Controller and processor**, and establishes significant obligations for both processor and controller in terms of data protection. One of the measures put forward by the GDPR in this aspect is data protection by design and default, a new approach that seeks to ensure that appropriate technical and organisational measures to protect personal data from the design stage of all new technology and to guarantee that processors collect as little data as possible in order to minimize any related risks. Along with that, this chapter establishes, in its articles 30, 32, 33, and 34, obligations for the processor in terms of recordkeeping, security, and communication with the data subject and the supervisory authority in case of a data breach. Measures such as these strive to not only reduce the risk of a data breach, as mentioned before, but also to mitigate the potential damage in the best way possible by notifying the competent authorities and the affected parties, which can allow the latter to take preventive measures against any issues.

In contrast with its predecessor, the GDPR establishes measures to fit new technologies into its framework by creating the 'data protection impact assessment' (DPIA) in article 35. For this purpose, both controllers and processors shall designate a Data Protection Officer (DPO) that will evaluate "personal aspects relating to natural persons which is based on automated processing"[68] with regards to any legal effects that the data processing might have. In case a

[67] Article 21, GDPR.

controller or processor fails to approve the DPIA, it can ask for the assistance of the supervisory authority in order to take the corresponding measures, as described in Article 36. Finally, articles 40 to 43 refer to the codes of conduct and the certification process, measures that should be encouraged by the member states but that are not mandatory, which at the very least allows data subjects to know which controllers and processors are trustworthy in the eye of the supervisory authority. The main purpose behind all the measures relating to this chapter would be, according to Mina and Schär, "to provide a more efficient and hassle-free monitoring, in an effort to ultimately render the European market more accessible for companies"[69] by providing standardized security measures and protocols that can be applied and enforced throughout the EU.

The third area of changes brought by the GDPR is the territorial scope of application of the regulation, which is detailed in chapter V. As the case of Schrems vs the Commissioner illustrated, the 1995 directive did not provide any type of protection for data subjects when their data was processed by companies outside the EU. This lead to the Safe Harbour agreement between the EU and the US, which was ultimately dismissed because of the Schrems case, proving the need to protect EU citizens' personal data from foreign companies and leading to the creation of this chapter. For this purpose, article 45 provides the guidelines for transfer of personal data to third countries or international organizations, which can only be done after the European Commission has determined that a specific country or organization offers the necessary protection. Some of the elements that the Commission considers for this decision are "the rule of law, respect for human rights and fundamental freedoms, relevant legislation,"[70] the existence of a supervisory authority within the country that enforces data protection rules or a

[68] Article 35, GDPR.
[69] Mina and Schär, p. 495 (2016).
[70] Article 45, GDPR.

supervisory authority that oversees the organization, and the international obligations in terms of data protection that the country or organization has acquired.

In case the Commission has not approved a certain country or organization for the transfer of personal data from the EU, a controller or processor may still do it if the latter can ensure an appropriate level of protection and the legal enforcement of the data subject's rights. Some of the mechanisms that can be used for this purpose are the previously mentioned code of conduct and certifications, along with binding corporate rules, legally binding and enforceable documents, and data protection clauses, among others. In addition to this, article 45 stipulates that decisions adopted by the Commission based on Article 25 of the 1995 Directive are still valid and should be monitored by the Commission in order to ensure that it still provides an adequate level of protection. Finally, data transfer to a third country or organization can still happen under certain circumstances even if the Commission has not approved it or if there are no data protection mechanisms in place. Some of these circumstances include the data subject consenting to the transfer of their data after being informed of the related risks,

The extensive nature of the GDPR is not only given by its 99 articles but also by the legal implications of these articles, as some might still be open to interpretation from national courts of justice and the EUCOJ. Probably the most comprehensive and accessible text explaining what the GDPR actually means in practical terms is Bussche and Voigt's *The EU General Data Protection Regulation: A Practical Guide*, which provides a checklist of obligations for both controllers and processors divided into two categories: organisational requirements and lawfulness of the processing activities. This checklist is included in the appendix for future reference.

# CHAPTER 3: DATA PROTECTION IN THE VIDEOGAME INDUSTRY: SOME CASES OF COMPLIANCE

This final chapter will delve into the current data protection protocols reflected by the privacy policies of five companies, which were selected based on brand recognition and revenue for the last quarter of 2019. The changes made to these policies in the last five years will be considered in order to measure the impact of the GDPR in the data protection standards for video game users, providing a qualitative analysis of these policies in order to draw conclusions about the advantages and disadvantages for users.

The effects of the GDPR application are not clear yet, even after two years of the regulation's entry into force, which could be attributed to a variety of reasons. The best example of this would be game developer Epic Games' data breach last year, when after an EU citizen requested access to the data Epic had on them it was sent to a different person, i.e. a third party.[71] Even though Epic, and the third party, assured the affected person that their information was deleted from the third party's computer, this was still a serious data breach under GDPR. On top of that, Epic's introduction of their own game launcher, a platform that allows players to buy and play games on their computers, received some criticism over their data collection, as the launcher accessed files in the players' computers without the players' consent, which was attributed by Epic's CEO Tim Sweeney to a rushed release of the software.[72] Despite cases like Epic's, there have been no fines issues to video game companies in Europe since the GDPR came into force, according to law firm CMS[73], which can be considered as an indicator of the industry's efforts to comply with the new regulations.

---

[71] Christou, Luke. "'Not so' Epic Games struggles with GDPR request --- has it breached data protection laws?" *Verdict.co.uk* (23 May 2019): https://www.verdict.co.uk/epic-games-gdpr-request/

[72] Mott, Nathaniel. "Epic Games Responds to Privacy Concerns About its Store." *Tom's Hardware* (16 March 2019): https://www.tomshardware.com/news/epic-games-responds-store-privacy,38835.html

[73] "GDPR Enforcement Tracker," *enforcementtracker.com.* https://www.enforcementtracker.com

In order to measure the impact that laws such as the GDPR have had on the video games industry and data protection protocols, the privacy policies of five different companies, both developers and publishers, will be analysed in terms of the noticeable changes during the last 5 years regarding data collection and processing, as well as users' rights. These companies were selected based on brand recognition, as is the case of **Valve Corporation** (also known as Valve[74]), owners of Steam which is a gaming platform with more than 20 million daily users; and revenue from quarter 4 of 2019[7576], as is the case of **Nintendo** ($2,286M), **Electronic Arts** ($1,593M), **Take-Two** ($930M), and **Ubisoft** ($510M).

### 3.1. Valve Corporation

Firstly, Valve's Privacy Policy from December 2015[77] states that users are agreeing to this policy and the collection and processing of their data just by using any of their services or products. In terms of the data collected, the policy refers to it as "personally identifiable information" as a synonym of personal data based on the meaning provided by Directive 95/46. The descriptions of the type of data being collected and its uses are rather vague, as there are no specifications about either topic, as the company has complete control of the user's data and the data subject has no control over their own information. Finally, Valve gave its users the choice to opt out of their mailing lists and the ability to request corrections, updates and removal of personal information, although these applications could be denied based on the company's discretion.

---

[74] "Steam and Game Stats" Steam, accessed 25 August 2020. https://store.steampowered.com/stats/
[75] "Gaming Revenue of Public Companies Worldwide in the 4th Quarter 2019," *Statista.* Last accessed: May 20, 2020. https://www.statista.com/statistics/983227/global-video-games-revenue-companies/
[76] "Top 25 Public Companies by Games Revenues," *Newzoo*, accessed 15 August 2020. https://newzoo.com/insights/rankings/top-25-companies-game-revenues/
[77] "Privacy Policy Agreement," *Steam*, accessed 20 July 2020. https://web.archive.org/web/20151212052350/http://store.steampowered.com/privacy_agreement/?l=english

The 2020 version of Valve's privacy policy[78] states that personal data is only collected if the user has provided their consent and if it is necessary for legal matters, purposes of the legitimate and legal interests of the company or a third party, and to provide its services. The types of data being collected and its sources are clearly outlined in this version of the policy and divided into 8 different categories: basic account data, transaction and payment data, other data the user explicitly submits, the data subject's use of the Steam client and websites, the subject's use of games and other subscriptions, tracking data and cookies, content recommendations, and information required to detect violations. These categories vary from personal information to financial information and predictive information, which includes game recommendations based on the users' interests and game activity. Along with this, the policy establishes that data will only be stored for as long as necessary and only for the purposes previously mentioned.

The most relevant changes to Valve's privacy policy can be observed in sections 5 and 6, which specify who has access to the user's personal data and the user's rights and control mechanisms respectively. With regards to third party access to the user's data, the policy explicitly states that Valve does not sell personal data and only shares data that is necessary for Valve to provide its services, something that is not mentioned in the 2015 version. Additionally, section 6 mentions legislations such as the GDPR and the California Consumer Privacy Act (CCPA) as the reasons behind Valve's decision to grant certain rights to their worldwide audience. These are the right of access, right to rectification, right to erasure, right to object, right to restriction of processing of personal data, right to personal data portability, and right to post-mortem control of your personal data, all of which were introduced and detailed in the

[78] "Privacy Policy Agreement"

GDPR except for the last one. Finally, the policy mentions Valve's compliance with the EU-US Privacy Shield Framework, which was recently taken down by the EUCOJ.[79]

### 3.2. Nintendo.

Nintendo's privacy policy from 2001[80] provides varied amounts of information regarding personal data by explaining the types of information the company collects, which include information provided by the user; information collected from the use of Nintendo's services and about the use of these same services; device, location, and purchases information; and the user's content. The next section of the policy refers to the different uses that the company gives to the data subject's information, such as the delivery, maintenance and improvement of their services, along with the use of cookies and website trackers to monitor the user's browser activity. The policy also explains when and with whom the user's personal data is shared, which refers mostly to third party service providers that complement Nintendo's own products. Finally, the last relevant point of the policy refers to the user's rights and control over their personal data, which the policy states may be offered and might "include the ability to update, correct or delete information that you have provided to us or information that we have collected through your use of our service."[81] Even though these choices are similar to the data subject's rights outlined in the GDPR, they are completely optional and the decision to allow the user to control their data lies ultimately on Nintendo alone.

The 2020 version of Nintendo's privacy policy[82] includes a few key changes that can be attributed to more strict laws such as the GDPR. This version of the policy describes the same

[79] Lomas, Natasha. "EU-US Privacy Shield is dead. Long live Privacy Shield," *TechCrunch* (11 August 2020): https://techcrunch.com/2020/08/11/eu-us-privacy-shield-is-dead-long-live-privacy-shield/
[80] "Nintendo Privacy Policy," *Nintendo* (March 2017): https://web.archive.org/web/20170303095428/http://www.nintendo.com/privacy-policy
[81] Section 4, Privacy Policy 2017.
[82] "Nintendo Privacy Policy"

categories of information collected and includes two new categories: information from third parties and aggregated and de-identified information, with the first category including information bought from third parties and the second referring to information that cannot be linked to an individual and is consequently not subject to the privacy policy. Section 2, which refers to how the company uses the information it collects presents one major change by including a paragraph explicitly stating that Nintendo does not sell the user's data, something that the user would not have known previously.

The third section of the privacy policy provides a more detailed account of how the user's data is shared in different scenarios, adding corporate affiliates and any scenario in which the user provides their consent to the ones listed in the previous policy. In terms of the data subject's rights, Nintendo's policy is more restrictive than Valve's, as it states that these rights are applicable depending on the user's place of residence, which means that users outside the European Union or the state of California might not be allowed to exercise these rights. Lastly, another relevant addition is the section regarding information retention, which did not exist in the previous version. Here, the policy states that the data subject's information "will be retained only for so long as reasonably necessary for the purposes set out in this privacy policy, in accordance with applicable laws"[83], once again implying that this might only apply to users from specific regions such as the European Union.

### 3.3. Electronic Arts

Electronic Arts' (also known as EA) privacy policy from 2016[84] begins in the same way as the previous two by outlining the information that the company collects, which includes

[83] Section 5, Privacy Policy 2020.
[84] "Privacy and Cookie Policy," *Electronic Arts* (28 November 2016): https://web.archive.org/web/20170710180348/https://www.ea.com/legal/privacy-policy

information provided by the data subject, information collected when one of the company's products is used, and information provided by third parties. In this last point, EA refers specifically to other video game companies such as Sony Entertainment, Microsoft, and Nintendo, as well as Facebook and Apple, as these third parties provide EA with the user's account information among other types of data. The second section of the policy outlines the ways in which EA collects information, which include cookies, different types of analytic technologies, ad serving technologies, and anti-cheat and fraud prevention technologies.

EA's policy explains in its third section how the company uses the user's data, which includes general purpose uses such as the operation of services, providing customer support, and personalization of communications. The fourth section refers to the data shared with third parties, which the company claims it does not do unless strictly necessary or after the user has given their consent. Additionally, the policy states that it also shares information with third parties who provide services to EA and that these third parties only use this data for the purposes stated in the policy. The next section explains that the user's data can be stored in any country in which the company operates and that the user willingly gives their consent to these data transfers by using EA's products even if the countries where the data is processed or stored does not provide the same level of data protection as the user's country of residence. Although this section mentions the US-Swiss Safe Harbor Framework, it does not mention the EU-US version of this agreement since it had been taken down the year before the publication of this policy.

Finally, this version of EA's policy outlines the user's choices and controls in section 8, which includes the ability for the user to opt out of mailing lists, update account preferences, deactivate their account, and delete and/or access their personal information. Interestingly, this version of the policy also mentions that the company "may request payment where allowed by

law"[85] before providing the user with their own data, something that could be considered as abusive practice and that was consequently removed in later versions of the document.

The 2020 version of EA's privacy policy[86] is divided into the same categories, with some small but relevant changes. In terms of the data collected by the company, new video game consoles have been included to third parties along with the legal basis for processing, in which it is established that the legal basis for processing the user's data presented in this section is the user's consent. In terms of how the company collects information, this version of the policy includes a subsection informing the player that third party advertising companies might use the information collected by EA in combination with information collected independently at their discretion, clarification that was not present in the 2015 version. The third section of the policy regarding how the company uses the user's information does not present any relevant changes as it refers to the same uses for this data.

One noticeable change in EA's privacy policy from 2016 to 2020 can be seen in section 4 regarding sharing the data subject's data with third parties. One of the additions to the later version is the fact that the company does not sell the user's information unless explicitly stated in the policy, which can be clarified by EA upon request. Additionally, this section provides a clearer presentation of the types of third parties that received the user's information by dividing them into categories such as affiliates, advertising partners, and service providers. The other section to present the biggest changes is the eighth, which refers to the user's choices and controls and not only presents the information in a more organized manner but also refers explicitly to the user's rights as established in the GDPR (rights to access, deletion, correction,

[85] Section 8, 2017 privacy policy.
[86] "Privacy and Cookie Policy," *Electronic Arts Inc.* (20 August 2020): https://web.archive.org/web/20200903230028/https://www.ea.com/legal/privacy-policy

and to opt out or object to certain processing). The clause that is present in the 2016 version, regarding EA's requiring users to pay a fee before accessing their own data has been deleted at some point in the last 4 years, which could certainly be attributed to tighter data protection laws.

### 3.4. Take-Two Interactive

Take-Two's privacy policy valid in January of 2016 was last updated in October of 2014, years before data protection and privacy laws were even announced. This version of the policy begins by warning the user that they are giving their consent just by registering for or using the companies' services, discarding immediately any possibility for the user to accept only specific clauses. In terms of its organization, this policy begins by explaining to whom and to which products it applies and directly naming the data controller for residents of the European Union. In this section it is also mentioned that the company may share the user's data with third parties such as service providers and social networking sites (referred to as SNS in the policy). Additionally, the policy explains that the company might harvest the user's gameplay information such "console ID, gaming service ID, game achievements, game scores and performance, IP address, MAC address, or other device ID, other console/device use information, or other information and statistics regarding your usage of the games"[87] without requiring the user's explicit consent.

After that, the policy explains different methods of passive data collection such as cookies, web beacons, log files, analytic metrics and advertising service providers, and it provides a list of different ad vendors and links to their respective privacy policies, while also letting the user know that they can opt out of certain targeted advertising lists. The policy then goes back to who collects the user's information and how it is used by explaining that certain

[87] Privacy Policy 2016, section 3.

identifiable information will be shared and made public after it has been collected, such as friend lists from SNS services like Facebook. The company may also share the user's data with third parties other than service providers, which includes law enforcement and/or governmental organizations, as well as in case the company deems it necessary to protect its interests or address any threats to itself. Finally, the policy refers to the data subject's ability to control and access their own data and it provides the necessary information for users to delete their accounts and personal data stored by the company, which the policy claims will only be stored as long as the account is active.

The 2020 version[88] of Take-Two's privacy policy presents some significant changes right from the start, as there is no longer a clause stating that the user consents to the policy as a whole like the one seen in the 2016 version. The newer version begins by describing the types of data collected and the legal bases for collecting it. Similar to the other companies mentioned, Take-Two collects information actively through the player when the latter provides it and passively through the use of their services and technologies (cookies, web beacons and log files). The type of data collected will depend on the data subject's use of these services and can include personal data, gameplay and console information, and information collected from third parties such as "public databases, console manufacturers, analytics providers, game developers, and other business partners that includes demographic information and information about your interests."[89] Additionally, this second section provides the legal basis for processing the user's data, which include the user's consent for specific purposes, in contrast with the all-purpose clause previously mentioned, legal requirements and the company's legitimate interests.

[88] "Take-Two Interactive Software Privacy Policy," *takes2games.com* (4 April 2020): https://web.archive.org/web/20200831234000if_/https://www.take2games.com/privacy
[89] Section 2, 2020 privacy policy.

The main uses for the data subject's data include providing and improving the company's services, fulfilling requests, communicating with and assisting the users, developing marketing studies and strategies, and to advertise different products. Some information can be used and made public even if the user has not registered for the company's services or given their consent, although this does not include any information that could identify the user. The next section of the policy details with whom the user's data is shared, which includes service providers, ad providers, and third parties during legal investigations, transfers of assets, and collaborative relationships. Additionally, the company may share aggregate or anonymous data with third parties for advertising purposes and it cannot be used to identify the user. The policy also outlines the user's rights regarding their data, which include opting in or out of email newsletters and personalized ad programs, objecting to having their data processed, and deleting, correcting or accessing their own data. Finally, this version of the policy adds a section about international transfers, which reflects a different level of protection for users from the EU through the use of Standard Contractual Clauses.

### 3.5. Ubisoft

The last of the five companies to be analysed is Ubisoft, whose privacy policy has been updated only twice in the last five years, in January of 2016 and in May of 2020. The active policy on February 2016[90] begins by describing its contents and claiming that by using the company's services, the user agrees to the terms of the policy, in a similar manner to Take-Two's. The first section explains when the company collects the user's data, which includes all interactions with the company, its products and its services. In terms of the type of data collected, the policy states that the company will only collect the information it considers to

[90] "Privacy Policy," *Ubisoft* (12 January 2016): https://web.archive.org/web/20160209203807/http://legal.ubi.com:80/privacypolicy/en-INTL

be "reasonably necessary to fulfil your requests and our legitimate business objectives."[91] The types of data collected include personal, demographic, and financial information collected from the users themselves along with data provided by third parties such as social networks, gaming platforms and other services. The policy also states that if a user refuses to provide their personal information they might not be able to access the company's services and products, which falls in line with the industry standards at that time.

The fifth section of Ubisoft's policy explains that some of the user's personal information might be made public through the public profile feature, but the user has some control over what information is displayed through this feature and who can access it and, consequently, the company is not responsible for the publication of this information. Regarding the means through which the user's data is collected, Ubisoft uses cookies, IP addresses, and other analytics tools in order to track the user's behaviour while using the company's services and products. The policy also explains that all the information collected through these means can be combined with personal data collected from other sources, which means it will then be subject to the terms explained in this policy. The seventh section refers to who collects the user's data, which includes Ubisoft and third party service providers, and how it is used, with its primary use being the provision of services and marketing purposes. Similarly, Ubisoft might share the data subject's information with third parties with the purposes of marketing and advertising different products to the user, features that can be disabled by the user at any time. Finally, the policy provides the information necessary for the user to question, view, correct and/or delete their personal information collected by the company with no extraordinary conditions. In case the user

[91] Section 1, privacy policy 2016.

wants their data to be deleted, the company reserves their right to keep some of the information for legal or technical purposes.

The 2020 version[92] of Ubisoft's privacy policy begins by explaining what is personal data, when it is collected and for what purposes. The information collected includes, similarly to the previous version of the policy, personal, demographic, and financial data provided by the user when creating a Ubisoft account, signing into the company's services through a social media login, making a purchase, using the company's games and services, and interacting with ads among other instances, and the main reasons behind the collection of these types of data are providing services and advertising Ubisoft's or third party products. Section 4 of this policy claims, similarly to the 2016 version, that personal data will be kept only for as long as necessary in order to fulfil its purpose, unless specified differently by law.

In terms of sharing the data subject's information, the policy claims it is shared with Ubisoft subsidiaries, third party service providers, advertising service providers, and administrative and judicial authorities. The next section explains the user's rights and how to exercise them, including the right of access and portability, right to rectification, right to object and withdraw consent, right to erasure, and right to restriction of processing, all of which are outlined and described in detail in the GDPR. Finally, the policy states that the company can use the user's data if there is a contract between the company and the user (represented by the Terms of Use of the Ubisoft Services), if it is in the company's legitimate interest, and if the user has given their consent, in stark contrast to the all-purpose consent clause present in the 2016 version.

[92] "Privacy Policy," *Ubisoft* (May 2020): https://web.archive.org/web/20200907221731/https://legal.ubi.com/privacypolicy/en-INTL

### 3.6. Advantages and disadvantages for users

Even though the changes introduced to the privacy policies of the five selected companies vary based on a multitude of factors, some trends can be identified and attributed directly to recent privacy and data protection laws such as the GDPR.

One of the main changes present in these policies is the understanding of consent and how it is given, as the older versions did not actively seek the user's consent to the policies' terms. This meant that users immediately agreed to the policies as a whole simply by using the companies' services or products without first being informed about these terms. Additionally, the policies relied on an all-purpose form of consent, which meant that most of the time users could not acquiesce with certain terms while withholding their consent to others, with the exception being mailing lists, as the option to unsubscribe from this feature precedes the latest privacy regulations. Consequently, the latest versions of the policies consider consent for each specific situation and the ability for users to choose when their personal data is being collected, as article 7 of the GDPR establishes that data controllers should be able to demonstrate that they have the user's consent in order to process their data. This change is reflected in all the analysed policies, and it can definitely be seen as an advantage for users in terms of controlling their own data.

The second trend of changes observed in all the analysed policies is the addition of the data subject's rights (right to access, delete, rectify, etc.) to these policies, as before 2018 these controls were mostly optional and the user's ability to exercise control over their own data was up to the companies themselves when they were available and there were no time constraints for the companies to comply with the user's requests. The one case that stood out in particular with regards to the user's controls was EA's, as the 2016 version of their privacy policy mentioned the possibility of charging users a fee in order to access their data, practice that could be

considered abusive and prohibitive for certain users. Even though these rights are now universal for companies operating in the European Union and the state of California and most users across the world can exercise them, some companies such as Nintendo have no legal obligation to provide these options to their users from regions other than the ones just mentioned, which the policy clearly states.

The last relevant change that can be observed in all the policies is related to transparency and ease of access to the policies themselves. All five of the policies analysed underwent aesthetic changes that made them easier to read and, consequently, understand its contents. Additionally, major changes were made to the policies with regards to the kind of information included in them. Some of the more relevant additions are the identification of the third parties with whom the user's data is shared, under which circumstances it is shared, how and when it is collected, and, most importantly, why it is being collected in the first place. Companies are also required to disclose whether they sell the user's identifiable data or not, which none of the five companies mentioned do. These changes can be directly attributed to laws such as the GDPR since it requires companies to justify their data collection and processing activities to the users so they can make an informed decision about their data.

These changes demonstrate that the GDPR has effectively increased the data protection standards of the video games industry as reflected in its protocols and privacy policies. This has meant the ability for users to make informed decisions about their data, to control their data even after it has been collected and processed by a company, and to access different products and services without the need to consent to abusive policies. Although some companies have adopted these practices and protocols on a global scale, ground-breaking legislation such as the GDPR has paved the way for other regions and countries to adopt similar data protection regulations.

Additionally, the articles relating to international data transfers are forcing the private sector to adopt minimum data protection standards, either by processing data in a country approved by the EU or by adopting Standard Contractual Clauses that guarantee a certain level of data protection for users.

# CONCLUSIONS

Data protection standards have evolved significantly over the last decades along with different technologies. Moreover, these technologies have changed enormously since the beginning of the century, which made regulations such as the EU's Data Protection Directive of 1995 fall behind. Along with that, the EU's single market needed a universal data protection framework that would standardize the national laws of its member states, which resulted in the creation of the GDPR in 2016. Its impact on the video games industry, which had a revenue of USD $13 billion in 2019, had not been analysed yet despite the fact that most video games currently require some form of data processing.

The first chapter characterised the video games industry as a global market that provides products and services to around 2.7 billion people while earning a total of around $109 billion in 2019. This userbase is quite diverse in terms of gender, age, and preferences, as both men and women of all ages play a wide variety of games in different platforms such as personal computers, video game consoles, and mobile phones. The last section of this chapter concludes that even though the video games industry has not had any cases of malpractice in the eyes of the European authorities, higher standards of data protection are an objective that should be constantly pursued.

The second chapter studied the evolution of data protection regulations in Europe from the data protection of 1981, passing through the data protection directive of 1995, and up until the GDPR in its current form. This study established clear differences between each regulation in terms of their form, content, and scope. In this sense, the GDPR can be seen as the byproduct of the continuous development of data protection regulation in Europe, as it has the broadest scope and higher standards of the three documents mentioned and studied.

As mentioned previously, this study set out to determine the effect of the GDPR on the video games industry by analysing the changes introduced to the privacy policies of five companies in the last five years. The analysis of these policies showed that the GDPR led to significant changes in the video games industry, introducing favourable changes for data subjects in terms of their rights, giving consent, and transparency, which means that users now have the tools to make informed decisions about their data in terms of who has access to their data and why it is being collected in the first place. Along with that, users from the EU now have more control than before over their own data as companies are obligated to respond to users' requests for data correction, deletion, portability, and access.

Based on this study, it can be stated that video game companies have adapted fairly well to the new regulation, as the analysis of five of the biggest video game companies of the world has shown. Even if the GDPR is only valid for companies operating within the EU, its effects can be seen on a global scale as companies from all over the world have to adapt to this regulation in order to operate in the European single market. This could mean that if other countries decide to adopt similar data protection laws, the impact on international companies will be lessened, which might encourage the adoption of these new standards in other regions.

# References

Arjoranta, Jonne. 2019. "How to Define Games and Why We Need to." *The Computer Games Journal* 109-120.

Christou, Luke, 2019. "'Not so' Epic Games struggles with GDPR request --- has it breached data protection laws?" Verdict.co.uk (23 May 2019): https://www.verdict.co.uk/epic-games-gdpr-request/

Council of Europe. 1981. "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data." Treaty, Strasbourg. Accessed May 18, 2020. https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37.

Court of Justice of the European Union. 2015. "The Court of Justice declares that the Commission's US Safe Harbour Decision is." Press Release, Luxemburg.

Electronic Arts, 2016. "Privacy and Cookie Policy," *Electronic Arts*. Last Modified 28 November 2016. https://web.archive.org/web/20170710180348/https://www.ea.com/legal/privacy-policy

Electronic Arts Inc., 2020. "Privacy and Cookie Policy," *Electronic Arts Inc*. Last Modified 20 August 2020. https://web.archive.org/web/20200903230028/https://www.ea.com/legal/privacy-policy

Enforcement Tracker. "GDPR Enforcement Tracker," *enforcementtracker.com*. https://www.enforcementtracker.com

Esposito, Nicolas. 2005. *A Short and Simple Definition of What a Videogame Is.* Centre de recherches, Compiègne: University of Technology of Compiègne.

European Union. 1995. "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data." Directive. Accessed May 18, 2020.

EUR-Lex, 2000. “Commission Decision,” *EUR-Lex.* Last Modified 26 July 2000. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32000D0520

EUR-Lex, 2000. “Commission Decision of 26 July 2000,” Official Journal of the European Communities. PDF. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ%3AL%3A2000%3A215%3A0007%3A0047%3AEN%3APDF#:~:text=Done%20at%20Brussels%2C%2026%20July%202000.&text=The%20European%20Union%27s%20comprehensive%20privacy,adequate%27%20level%20of%20privacy%20protection.

EUR-Lex, 2012. “Charter of the Fundamental Rights of the European Union,” *Official Journal of the European Union*. Last Modified 26 October 2012. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:12012P/TXT

EUR-Lex, 2014. “Judgment of the Court (Grand Chamber),” *EUR-Lex*. Last Modified 8 April 2014. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293

EUR-Lex, 2014. “Judgment of the Court (Grand Chamber),” *EUR-Lex*. Last Modified 13 May 2014. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131

Fair, Lesley. 2017. *What Vizio was doing behind the TV screen.* Federal Trade Comission. https://www.ftc.gov/news-events/blogs/business-blog/2017/02/what-vizio-was-doing-behind-tv-screen.

Fromholz, Julia M. 2000. "The European Union Data Privacy Directive." *Berkeley Technology Law Journal* 15 (1): 461-484. Accessed May 18, 2020.

Gilbert, Francoise. 2007. "A Bird's-Eye View of Data Protection in Europe." *GPSolo* (American Bar Association) 32-35.

Interactive Software Federation of Europe. n.d. *About ISFE.* Accessed May 2020, 18. https://www.isfe.eu/about-ifse/.

Interactive Software Federation of Europe. 2019. "Key Facts 2019." PDF.

Lomas, Natasha, 2020. “EU-US Privacy Shield is dead. Long live Privacy Shield,” TechCrunch (11 August 2020): https://techcrunch.com/2020/08/11/eu-us-privacy-shield-is-dead-long-live-privacy-shield/

Melendez, Steven and Alex Pasternack, “Here are the data brokers quietly buying and selling your personal information”, Fast Company, 2019 https://www.fastcompany.com/90310803/here-are-the-data-brokers-quietly-buying-and-selling-your-personal-information

Mina, Burri, and Rahel Schär. 2016. "The Reform of the EU Data Protection Framework: Outlining Key Changes and AssessingTheir Fitness for a Data-Driven Economy." *Journal of Information Policy* (Penn State University Press) 6: 479-511.

Mott, Nathaniel, 2019. “Epic Games Responds to Privacy Concerns About its Store.” Tom’s Hardware (16 March 2019): https://www.tomshardware.com/news/epic-games-responds-store-privacy,38835.html

Newzoo, 2020. “Top 25 Public Companies by Games Revenues.” *Newzoo*. Accessed 15 August 2020. https://newzoo.com/insights/rankings/top-25-companies-game-revenues/

Nintendo, 2017. “Nintendo Privacy Policy,” *Nintendo*. Last Modified March 2017. https://web.archive.org/web/20170303095428/http://www.nintendo.com/privacy-policy

Russell, N. Cameron, Joel R Reidenberg, and Sumyung Moon. 2018. *Privacy in Gaming.* New York: Center on Law and Information Policy.

Statista. n.d. *Video Games - Europe: Statista Market Forecast.* Accessed May 18, 2020. https://www.statista.com/outlook/203/102/video-games/europe#market-users.

Steam, 2020. “Privacy Policy Agreement.” *Steam*. Accessed 20 July 2020. https://web.archive.org/web/20151212052350/http://store.steampowered.com/privacy_agreement/?l=english

Steam, 2020. “Estadísticas de Steam y de los Juegos.” *Steam*. Accessed 25 August 2020. https://store.steampowered.com/stats/

SuperData. 2020. *2019 Year in Review.* PPT Presentation, SuperData.

Takes2Games, 2020. “Take-Two Interactive Software Privacy Policy,” *takes2games.com*. Last Modified 4 April 2020. https://web.archive.org/web/20200831234000if_/https://www.take2games.com/privacy

Ubisoft, 2016. “Privacy Policy,” *Ubisoft*. Last Modified 12 January 2016. https://web.archive.org/web/20160209203807/http://legal.ubi.com:80/privacypolicy/en-INTL

Ubisoft, 2020. “Privacy Policy,” *Ubisoft*. Last Modified May 2020. https://web.archive.org/web/20200907221731/https://legal.ubi.com/privacypolicy/en-INTL

Warren, Samuel D., and Louis D. Brandeis. 1890. "The Right to Privacy." *Harvard Law Review* 4 (5): 193-220. Accessed May 18e, 2020. doi:10.2307/1321160.

Appendix

**Definitions given by the EU's Convention, Directive and Regulation.**

| | |
|---|---|
| **Personal data** | |
| Convention | Any information relating to an identified or identifiable individual ("data subject"). |
| Directive | Any information relating to an identified or identifiable natural person ("data subject"). |
| GDPR | Any information relating to an identified or identifiable natural person ("data subject"). |
| **Data subject** | |
| Convention | An identified or identifiable individual. |
| Directive | An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. |
| GDPR | An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. |
| **Automated data file** | |
| Convention | Any set of data undergoing automatic processing. |
| Directive | Not defined. |
| GDPR | Not defined. |
| **Automatic processing/processing of personal data/processing** | |
| Convention | 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. |
| Directive | Any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction |

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

| **Restriction of processing** | |
|---|---|
| Convention | Not defined |
| Directive | Not defined |
| GDPR | The marking of stored personal data with the aim of limiting their processing in the future. |

| **Profiling** | |
|---|---|
| Convention | Not defined |
| Directive | Not defined |
| GDPR | Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. |

| **Pseudonymisation** | |
|---|---|
| Convention | Not defined. |
| Directive | Not defined. |
| GDPR | Processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person |

| **Filing system** | |
|---|---|
| Convention | Not defined. |
| Directive | Not defined. |
| GDPR | Any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis |

| | |
|---|---|
| **Controller of the file/controller** | |
| Convention | The natural or legal person, public authority, agency or any other body who is competent according to the national law to decide what should be the purpose of the automated data file, which categories of personal data should be stored and which operations should be applied to them. |
| Directive | The natural or legal person, public authority, agency or any 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 processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law. |
| GDPR | 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** | |
| Convention | Not defined. |
| Directive | A natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller. |
| GDPR | A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller |

| | |
|---|---|
| **Third Party** | |
| Convention | Not defined. |
| Directive | Any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data. |
| GDPR | A natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data |

| | |
|---|---|
| **Recipient** | |
| Convention | Not defined. |
| Directive | A natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients. |

| | |
|---|---|
| GDPR | A natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing |
| **The data subject's consent/consent** | |
| Convention | Not defined. |
| Directive | Any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed. |
| GDPR | Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. |
| **Personal data breach** | |
| Convention | Not defined. |
| Directive | Not defined. |
| GDPR | A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed |
| **Genetic Data** | |
| Convention | Not defined. |
| Directive | Not defined. |
| GDPR | Personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question |
| **Biometric data** | |
| Convention | Not defined. |
| Directive | Not defined. |
| GDPR | Personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural |

| | |
|---|---|
| | person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data |
| **Data concerning health** | |
| Convention | Not defined. |
| Directive | Not defined. |
| GDPR | Personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status |
| **Main establishment** | |
| Convention | Not defined. |
| Directive | Not defined. |
| GDPR | (a) as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment.<br>(b) as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation. |
| **Representative** | |
| Convention | Not defined. |
| Directive | Not defined. |
| GDPR | A natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Regulation. |
| **Enterprise** | |
| Convention | Not defined. |
| Directive | Not defined. |

| | |
|---|---|
| GDPR | A natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity. |

| **Group of undertakings** | |
|---|---|
| Convention | Not defined. |
| Directive | Not defined. |
| GDPR | A controlling undertaking and its controlled undertakings. |

| **Binding corporate rules** | |
|---|---|
| Convention | Not defined. |
| Directive | Not defined. |
| GDPR | Personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity. |

| **Supervisory authority** | |
|---|---|
| Convention | Not defined. |
| Directive | Not defined. |
| GDPR | An independent public authority which is established by a Member State pursuant to Article 51. |

| **Supervisory authority concerned** | |
|---|---|
| Convention | Not defined. |
| Directive | Not defined. |
| GDPR | A supervisory authority which is concerned by the processing of personal data because.<br>(a) the controller or processor is established on the territory of the Member State of that supervisory authority;<br>(b) data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or<br>(c) a complaint has been lodged with that supervisory authority. |

| | |
|---|---|
| **Cross-border processing** | |
| Convention | Not defined. |
| Directive | Not defined. |
| GDPR | (a) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or<br>(b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State. |
| **Relevant and reasoned objection** | |
| Convention | Not defined. |
| Directive | Not defined. |
| GDPR | An objection to a draft decision as to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union |
| **Information society service** | |
| Convention | Not defined. |
| Directive | Not defined. |
| GDPR | A service as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council. |
| **International organisation** | |
| Convention | Not defined. |
| Directive | Not defined. |
| GDPR | An organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries. |

**GDPR Checklist by Bussche and Voigt.**

- **Organisational requirements**
    - Records of processing activities.
    - Designation of a Data Protection Officer.
    - Data protection impact assessment.
    - Data protection by design and by default.
    - Technical and organisational measures.
    - Data subject rights.
    - Data breach notification.
    - Data protection management system.
    - Appointment of a representative by non-EU entities.
    - Codes of conduct and certifications.
- **Lawfulness of the processing activities.**
    - Legal bases for processing.
    - Intra-group processing activities.
    - Special categories of personal data.
    - Involvement of a processor.
    - General requirements for third country data transfers.
    - EU standard contractual clauses.
    - EU-US privacy shield.
    - Binding corporate rules.