INTERNATIONAL JOURNAL OF
SCIENCE ARTS AND COMMERCE

Protecting Children's Personal Data in a Video Game Environment

Maria-Alexandra Enescu

- Related subject/Field (Branch of study): Data protection, Data Law
- Title of the paper: Protecting Children's Personal Data in a Video Game Environment
- Author name(s): Maria-Alexandra Enescu
- Designation: Independent legal researcher
- Department: Law
- Institute/University: Institute of European Studies – Vrije Universiteit Brussel
- State: Brussels
- Country: Belgium
- Address: Duprestraat 94, 131, 1090 Jette
- Phone number: +40736784333
- E-mail address: enescu_maria96@yahoo.com

Author's biography:

Maria-Alexandra Enescu is a Romanian lawyer, who successfully completed an LL.M in International and European Law, with a Data Law specialization, at the Institute for European Studies (VUB). She authored a Master's thesis on the same topic as this article and issued an online course on how parents can protect their children online, aiming to contribute to a safer online environment, especially from a data protection perspective. She is particularly interested in the legal implications of the newest technologies. As a result, she created a legal blog, TECH&LAW ON THE GO. She also took part in the ELSA Advocacy project on Data Protection, concerning the tracing systems in Belgium.

Abstract

This article focused on the correlation between the video game industry and the children's right to privacy and to the protection of their personal data. The research was conducted through the lens of, but not limited to, the General Data Protection Regulation as the main legal instrument aiming to grant an increased level of protection to children. It analysed the legal implications of this developing industry, assessing whether the available legal framework is prepared to address the issues that may stem from video games and other adjacent emerging technologies. In order to limit the scope of the paper, Massively

Multiplayer Online Role-Playing Games were chosen as a main focus. The main objective of the paper was to find relevant and practical recommendations for effectively securing children's interests, that might be abused by video game companies, while ensuring the realization of other rights of the child, such as the freedom of expression, the freedom of assembly and the right to education and recreation, granted by The United Nations Convention on the Rights of the Child. These recommendations are addressed to all of the stakeholders (relevant national authorities, supervisory authorities, video game companies, parents and children themselves). A multi-stakeholder approach to this issue would significantly increase the efficiency of these recommendations.

Keywords: Children, video games, MMORPG, data protection, fundamental rights, rights of the child, GDPR.

Abbreviations:

MMORPG: Multiplayer Online Role-Playing Games

GDPR: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (The General Data Protection Regulation)[1]

UNCRC: United Nations General Assembly, 'Convention on the Rights of the Child'[2]

WP29: Article 29 Working Party

1. Introduction

Children's right to data protection and online privacy has been a widely debated topic among lawyers, legislators, and researchers. The importance of this topic is undeniable, considering the vulnerability, the lack of knowledge and experience of the youngest members of our society.

The novelty of this paper resides, however, in exploring the correlation between data protection and online privacy, on the one hand, and Massively Multiplayer Online Role-Playing Games (MMORPGs), on the other hand, considering their complexity and their undeniable resemblance with the real world.

Therefore, this research will be conducted having the MMORPGs as a primary focus. The conclusions that will have been drawn by the end of this paper by analysing a range of privacy

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data [2016] OJ L119/1

[2] UN General Assembly, 'Convention on the Rights of the Child',1989, United Nations, Treaty Series, vol. 1577, p. 3

issues concerning MMORPGs could be further extended to the broader notion of "video games".

In this context, a plethora of privacy issues may arise in a video game environment, such as: privacy policies not complying with the existing data protection laws, processing of an enormous amount of personal data, including sensitive and biometric data, data security breaches, unlawful advertising techniques, unlawful profiling, and many others. Nevertheless, with reasonable diligence, proper understanding of the legal consequences of one's actions, and resorting to the available safeguards, an adult could avoid becoming the victim of unlawful data processing.

However, if a child is involved, a more cautious approach is required. It is no secret that children are regular consumers of video game companies' services, which might lead to "risks related to personal data misuse or abuse"[3] considering that game companies regard children as a "data source"[4], contributing to the phenomenon of what has been tagged as "datafication" and "dataveillance" of children[5], considering that children-related information in terms of "their bodies, play and social interactions"[6] is of great economic value and can be easily exploited.

While the "digital realm"[7] operators are providing children with the most engaging, interactive and entertaining activities, they are, simultaneously, collecting vast amounts of data, "either surreptitiously or with the consent of children or parents"[8]. Therefore, additional safeguards and special protection measures[9] are necessary when children are involved, because they are not always able to consent or to predict the consequences of their consent[10].
The seven chapters are laid out to answer the following <u>*research question*</u>: *how can children be protected against abusive personal data processing performed by video game companies, and, in particular, by MMORPG providers?*

2. Background

2.1 Definitions

A *video game* is an electronic game based on the interaction between the user and the user interface, to generate visual feedback on a video display device, either it be a computer

[3] S van der Hof, 'No Child's Play: Online Data Protection for Children' in S van der Hof, Van den Berg B, Schermer B (eds) *Minding Minors Wandering the Web: Regulating Online Child Safety* (Springer 2014).
[4] D Holloway, 'Surveillance Capitalism and Children's Data: The Internet of Toys and Things for Children' (2019) 170 Media International Australia 27 <http://journals.sagepub.com/doi/10.1177/1329878X19828205> accessed 4 March 2020.
[5] D Lupton and B Williamson, 'The Datafied Child: The Dataveillance of Children and Implications for Their Rights' (2017) New Media & Society, 19(5) 780-794 <https://doi.org/10.1177/1461444816686328> accessed 14 February 2020.
[6] D Holloway (n 5).
[7] ibid.
[8] ibid.
[9] van der Hof (n 4).
[10] Lupton and Williamson (n 6).

screen, a TV set, a smartphone touchscreen, or a virtual reality headset. This interaction is performed via a controller, which translates the user's actions into in-game actions. The controller can take several forms, ranging from the well-known mouse and keyboard to touchscreens, digital cameras, and even motion sensors.[11]

Massively Multiplayer Online Roleplaying Games are placed, at the interference between computer and console games, as they can be played both on a PC or on a game console, such as Xbox, Switch or PS4. They distinguish themselves from other video games by allowing their numerous players to interact with one another within a virtual world, in real time. The concept of "virtual world", which characterizes MMORPGs, has been defined as "a synchronous, persistent network of people, represented as avatars"[12], that cooperate and communicate in the context of a virtual environment, which, through its qualities, might resemble a real-world society.

2.2 The Correlation between MMORPGs and Data Protection Laws

To begin with, the functioning of an MMORPG is fairly simple to understand, as it can be summarized in four stages: creating the account, downloading the game, choosing an avatar, and playing. To be more specific, players, who are represented in the game by an avatar, whose external appearance is designed by the platform provider[13], enter into a three-dimensional virtual world that is theirs to explore.[14] In this context, they progress by "acquiring skills and possessions, interacting and collaborating"[15] with other players for completing the game's tasks and objectives.

It can be anticipated that all of these four stages imply certain data processing. In addition to several foreseeable categories of personal data that are usually collected in the context of a video game, such as the player's real name, email address, phone number, age, bank details (if the game is paid for or products are purchased during the game) and other online identifiers, video game companies collect certain categories of personal data which might pose the player's privacy at risk, in particular if the data subject is a child.

Therefore, there other various other types of data that can constitute "personal data" or even "sensitive personal data"[16] (such as sexual life, sexual orientation, health, or mental health) that might be collected from players, falling under the scope of data protection laws.

---

[11] J Newman, I Simons and E Jarvis, *Difficult Questions about Video Games* (Suppose Partners 2004).
[12] J Comas and F Tschang, 'The Brief History, Tumultuous Present and Uncertain Future of Virtual Worlds (Terrae Fabricatae)' in S Hotho, N McGregor(eds) *Changing the Rules of the Game: Economic, Management and Emerging Issues in the Computer Games Industry* (Palgrave Macmillan 2013).

[13] B Schafer and W Abel, 'All the World's a Stage — Legal and Cultural Reflections on the Surveillance of Online Games' (2014) 38 Datenschutz und Datensicherheit - DuD 593-600.
[14] V A Badrinarayanan, J J Sierra and K M Martin, 'A Dual Identification Framework of Online Multiplayer Video Games: The Case of Massively Multiplayer Online Role Playing Games (MMORPGs)' (2015) 68 Journal of Business Research 1045.
[15] ibid.
[16] Schafer and Abel (n 14).

2.2.1 Types of Data whose Processing Might Raise Particular Concerns

"In-game data" is data collected while the child is playing and is represented by the player's in-game choices, the customization of their avatar and the inter-player interactions. This data, once compiled and analysed, can contribute to the creation of a detailed profile of the user.

First of all, *the player's in-game choices and activities* represent a transposition of the human controlling the avatar into the game environment. By analysing this behaviour, a detailed profile of the individual can be portrayed. To illustrate, the abilities and actions the players choose for their character can be indicators of their real-life jobs. Also, the chosen class for the avatar can reflect their personalities; one player can choose to directly involve into battles, whereas another can choose to help others restore their strength; some might choose to fight alone, while others choose to involve in group activities or be part of a guild. In addition, choosing the magical abilities can be regarded as an indication of the player's interests; for example, a person interested in medicine might choose to be a healer within the game.[17]

Secondly, the *avatar* is relevant for the correlation with data protection law from two perspectives: the avatar's in-game behaviour and the avatar construction.

From an avatar's conduct perspective, the individual behind it can be easily identified, given that the player's log-in credentials are "uniquely and persistently linked to the avatar"[18]. The platform provides access to the avatar only after recognizing the credentials, attributing a "stable identity"[19] to the player. Therefore, this avatar's behaviour can be attributed to an identifiable person, exactly like "filming a human on CCTV"[20]. The avatar is identified in the game by other players by its pseudonym, but, at the same time, by the real person's behaviour, choices or interactions.

From an avatar construction perspective, most of the available MMORPGs cater for a wide range of customization options that allow the players to design an avatar that either significantly resembles their real-world appearance, or depicts how they see themselves. Or, even if the design they choose does not correspond to their offline body or identity, it is still considered to be "part of it"[21]. More precisely, for customizing an avatar, players must choose: a race (either gnome, human, elf, dwarf), a gender, a class (warrior, healer, mage, scout), clothing, accessories, hair, skin tone, facial features, height, weight, and, most recently, they even have the possibility to choose a sexual orientation (straight, gay or bisexual). The latter feature has been adopted, for instance, by the MMORPG Dragon Age II[22].

[17] Badrinarayanan, Sierra and Martin (n 15).
[18] ibid.
[19] ibid.
[20] ibid.
[21] D Nielsen, 'Identity Performance in Roleplaying Games' (2015) 38 Computers and Composition 45.
[22] ibid.

Therefore, MMORPGs encourage ”identity play”.[23]

Another similarity between the virtual and the real world is that the avatar, just as the human behind it, might change over time, acquiring better equipment, clothing or assets, or even experiencing a virtual aging process.[24] Therefore, the avatars are considered personal data for the purposes of data protection laws.

Another factor that contributes to the players' profiling is represented by their *in-game interactions*; by monitoring chat rooms, the video game company can learn if a player is aggressive or peaceful, literate or illiterate, a follower or a leader.

Additionally, the in-game chat and calls are of particular interest from a data protection perspective as well. If, initially, these facilities were implemented to create the framework for users to communicate for attaining the game's objectives, it is a well-known fact that most players use them to socialize, affirming that this is "one of the most appealing aspects of playing MMORPGs"[25]. Consequently, these communications are extremely dense in personal information, often containing enormous amounts of sensitive data.

"Real-world data" is collected if the game account and the player's social media account (such as their Facebook account) are linked. In this case, data such as cookies or the location of the player exploiting the GPS or IP function might be processed. All this data is often used, in addition to improving the player's experience and the service itself, for profiling children and providing behavioural advertising.

Sensitive data/ special categories of data, as they are defined by Article 9 of the GDPR, are represented, in the context of an MMORPG, by data relating to sexual life, sexual orientation and data on physical or mental health. On the one hand, this data can be extracted from inter-player interactions, as we have already seen, through the in-game chat or other communication mechanisms, such as in-game calls, using a microphone and, eventually, a video camera.

Of course, all these interactions are stored by the game platform, or can be followed even in real time by an employee of the game, which monitors conversations between players[26], theoretically in order to prevent and combat disrespectful behaviour or vocabulary towards other players (such as the use of inappropriate language or harassment) or illegal conduct according to the rules of the game (using hacks or trolling other players).

[23] ibid.
[24] Schafer and Abel (n 14).
[25] ibid.
[26] Jürgen Bänsch, 'CPDP 2020', *Children's privacy in the digital age* (2020) <https://www.youtube.com/watch?v=2ss-Q88YHEE>.

On the other hand, the game platform can come into possession of sensitive data of children by profiling them, based on their in-game behaviour or choices. For example, regarding mental health data, excessive presence in the game may indicate an addiction.[27]

Biometric data, also falling under the scope of Article 9 of the GDPR, can be collected via various sensors that are increasingly integrated into gaming consoles, such as Xbox and Playstation, which are gaining in popularity among children. To exemplify, facial recognition sensors might be utilized for game authentication; other sensors might be incorporated for capturing voice, in order to respond to voice commands or to detect profanity words; motion sensors, which accurately capture body movements , transposing them into the game environment, represent the newest feature that show us that the future is now.

3. Applicable Normative Framework

This chapter's objective is to identify the normative framework applicable to video game companies processing personal data of children; as there is no law governing the video game industry itself[28] the most relevant legal instruments were selected.

3.1 The United Nations Convention on the Rights of the Child29 (UNCRC)

UNCRC promptly begins with a clear definition of a child, as any human being below the age of 18, unless the majority is attained earlier.[30] However, the principle of "the best interests of the child"[31] , as fundamental as it might be, remains pretty obscure, as "there is no unanimously accepted standard"[32] for what it implies. Both public and private social welfare institutions (including video game companies), should be concerned with the respect of this principle. Researchers[33] have tried to interpret it by classifying the children's rights under UNCRC into three categories: protection rights, provision rights and participation rights.

Firstly, *protection rights* refer to protecting children against neglect and abuse.[34] In this context, children are granted a right to privacy[35], which includes the protection of personal data[36]. The UNCRC encourages parents in their child upbringing responsibilities[37], by

[27] J Newman, J Jerome and C Hazard, 'Press Start to Track? Privacy and the New Questions Posed by Modern Videogame Technology' [2014] American Intellectual Property Law Association (AILPA) Quarterly Journal 1.
[28] S Blickensderfer and NA Brown, 'S1:E3 - Even the Games Have Eyes: Data Privacy and Gaming | Carlton Fields' (2019) <https://www.carltonfields.com/insights/podcasts/lan-party-lawyers/games-have-eyes-data-privacy-gaming> accessed 4 March 2020.
[29] Convention on the Rights of the Child (n 3).
[30] Art. 1 of the UNCRC
[31] Art. 3 of the UNCRC
[32] S Livingstone and B O'Neill, 'Children's Rights Online: Challenges, Dilemmas and Emerging Directions' Children' in S van der Hof, Van den Berg B, Schermer B (eds) *Minding Minors Wandering the Web: Regulating Online Child Safety* (Springer 2014).
[33] ibid.
[34] ibid.
[35] Art. 16 of the UNCRC
[36] van der Hof (n 4).
[37] Art. 18 of the UNCRC

promoting "the use of parental controls and filters on devices and platforms"[38]. However, parents' interference should be balanced with the child's right to privacy and to "preserve his or her identity"[39] while playing a game.

Secondly, *provision rights* refer to the fulfillment of the basic needs of the child. Applicable in the context of video games are the articles[40] refering to the right to education and recreation. By playing video games, both of these rights are realized to a certain extent. Regarding the right to education, while playing, the child develops digital competence, which represents a contemporary component of this right.[41] Video games might also encourage the realization of the right to leisure appropriate to their age and might facilitate the development of certain skills, such as social skills or resilience to attain the game's tasks. Therefore, children should not be prohibited the access to video games, but their access should be carefully controlled.

Thirdly, *participation rights* stand for children's active participation in their families and communities. Children have the right to form and express their own view in matters directly affecting them, according to their age and level of maturity.[42] In the context of video games, there might be situations when children have a deeper understanding of the digital environment and can significantly contribute to making a decision, alongside with their parents, such as expressing consent to the processing of their personal data. Freedom of expression[43] is also relevant; by designing an avatar, chatting with other players, contributing to the game community with their ideas and game tips, or being active on the game forum, children have the opportunity to express themselves. In addition to this, they are granted freedom of assembly[44] which is reflected in associating with other players in the form of a guild or other unions, for succeeding in game.

3.2 The General Data Protection Regulation (GDPR)

At an EU level, the GDPR is by far the main legal instrument regulating personal data processing performed by video game companies and protecting children against abusive and unlawful data processing.

To begin with, it can be observed that the scope of the GDPR is fairly extended. Regarding its territorial scope, it applies to any company located in the EU or providing services to people located in the EU.[45] Therefore, considering that the gaming industry is a significant market in the EU, the GDPR applies to virtually every video game provider[46], even if most of them are located outside of the EU.

[38] Livingstone and O'Neill (n 33).
[39] Art. 8 of the UNCRC
[40] Art. 28, 29, 30 of the UNCRC
[41] Livingstone and O'Neill (n 33).
[42] Art. 12 of the UNCRC
[43] Art. 13 of the UNCRC
[44] Art. 15 of the UNCRC
[45] Art. 3 of the GDPR
[46] T Wessing, A Hartlaub and B Stach, 'Data Protection and Games ' Taylor Wessing PlugIn (July 2019) <https://iot.taylorwessing.com/data-protection-and-games/> accessed 4 March 2020.

Regarding the material scope concerning children, the Regulation applies to "information society services directly offered to a child"[47] which involve the processing of their personal data. These services have been defined as "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient"[48]. It has been stated[49] that the so-called "free services", which are, in reality, services that are financed by advertising, should be caught under the scope of this definition. Therefore, video games, either they charge a monthly subscription or they are "free" can be considered "information society services". However, the meaning of "service offered directly to a child" remains rather unclear, as it could refer both to services that are targeted at children or services that are actually used by children, even if they are targeted at adults[50]. Of course, MMORPGs fall under the scope of the second interpretation and it is clear that, should the first interpretation be adopted, the special protection granted to children under Article 8 would be undermined.
An aspect that merits specific attention is a child's lawful age of consent. According to the GDPR, the processing of personal data is lawful if the child is above 16 years of age.[51] If the child is below this threshold, parental consent or authorization is required. However, each Member State is given the possibility to lower this age down to 13. In addition to this freedom of decision, the law of contracts of each Member State will apply concerning the validity, the formation, and the effects of a contract in relation to a child. Needless to mention, this leads to a discontinuous interpretation of a contract between a child and a video game company, hence the difficulty to assess the lawfulness of the contract performed according to the law of the Member State where the child resides.

If the child is under-aged and, thus, unable to express a valid consent to the processing of their personal data, parental consent is required, as a safeguard for protecting the child's online privacy. However, this consent might sometimes be insufficient, as the parent's surveillance over the child might be difficult to ensure. A balance needs to be struck between parent's surveillance and child's freedom of expression and freedom to make mistakes and to learn, as laid out in the UNCRC. This parental supervision needs to be sufficient, efficient, but proportionate.[52] Otherwise, excessive interference could constitute another breach of the child's right to privacy.[53] Moreover, if parents experience difficulties in understanding the digital environment, especially regarding MMORPGs, it is questionable whether their consent is given in full knowledge of the facts and whether it is veritably valid.

[47] Art. 8 of the GDPR
[48] Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services [2015] *OJ L 241*
[49] E Lievens and V Verdoodt, 'Looking for Needles in a Haystack: Key Issues Affecting Children's Rights in the General Data Protection Regulation' (2018) 34 Computer Law & Security Review 269 <https://linkinghub.elsevier.com/retrieve/pii/S026736491730314X> accessed 4 March 2020.
[50] ibid.
[51] Article 8 of the GDPR
[52] S Livingstone, 'CPDP 2020', *Children's privacy in the digital age* (2020) <https://www.youtube.com/watch?v=2ss-Q88YHEE&t=2745s>.
[53] Lievens and Verdoodt (n 50).

When parental consent is given, the GDPR imposes an obligation on the controller and, thus, on video game companies, to make ”reasonable efforts” to verify if it is lawful, by resorting to the available technology.[54] However, there is no unanimously accepted definition of these two concepts (”verifiable parental consent” and ”reasonable efforts”). This legal uncertainty creates a burden for video game companies regarding the circumstances under which such consent is required, risking either to provide insufficient protection for children or excessive intervention from their parents, limiting their online freedom.[55]

The GDPR imposes a variety of obligations on controllers, including video game companies. They have to comply with the principles of purpose limitation, data minimization, storage and temporal limitation, integrity, and confidentiality of data.[56] The special protection granted to children by this legal instrument is reflected in this area as well. Taking into account their vulnerability, WP29[57] argued that these principles should be interpreted more strictly when the service is aimed at children, especially concerning the principles of data minimization and purpose limitation.[58] Data minimization can be achieved by ensuring a ”privacy-by-design”[59] approach, through techniques such as pseudonymization, while purpose limitation can be ensured by a ”privacy-by-default”[60] approach, which entails that the default settings should offer the highest level of protection of personal data. It has been affirmed[61] that the GDPR strengthens the role of these principles, ensuring more efficient data protection and increasing the accountability of data controllers.

Another obligation of video game companies is to justify the lawfulness of the processing operations[62]. Usually, they resort either to ”consent” or to ”legitimate interest” as their legal basis. On the one hand, relying on a child’s consent as a sole basis might not be the best approach due to its uncertain validity. On the other hand, regarding legitimate interest, it has been stated[63] that the interests of the video game company can be overridden more easily by the interests of the child rather than by those of an adult. This aspect is particularly relevant in the sphere of profiling children for marketing purposes, which places a great responsibility on video game providers to balance their interest of direct marketing with the rights and freedoms awarded to a child player; this creates another source of legal uncertainty.[64]

If adults are targeted by these techniques, they have the right to object at any time to the processing for marketing purposes[65], but the question that arises is whether such a safeguard

[54] Art. 8 of the GDPR
[55] van der Hof (n 16).
[56] Art. 5 of the GDPR
[57] Article 29 Working Party, now replaced by European Data Protection Board (EDPB)
[58]Article 29 Data Protection Working Party, ‘Opinion 02/2013 on Apps on Smart Devices’ [2013]
[59] Art. 25 of the GDPR
[60] Ibid.
[61] L A Bygrave, ‘Data Protection by Design and by Default : Deciphering the EU’s Legislative Requirements’ (2017) 1 Oslo Law Review 105.
[62] Art. 6 of the GDPR
[63] Lievens and Verdoodt (n 50).
[64] ibid.
[65] Art. 21 of the GDPR

suffices when the subject of the profiling is a child. WP29 stated that children's data should not be used for behavioral advertising purposes, directly or indirectly; if video game companies adopt this technique, the processing is considered to be unlawful, exceeding the understanding capacities of the child.[66] For reducing the risks for children's privacy, "a higher degree of responsibility and accountability" is recommended to video game providers in case of child profiling.[67] As can be observed, the WP29 guidelines, even if this body no longer exists, still represent valuable resources to be resorted to for clarifying certain obscure provisions of the GDPR and most of them have been embraced by the actual EDPB.[68]

Adding to the special protection granted to children, it is recommended that profiling based "solely on automated processing should not concern children"[69] as long as this produces legal or other significant effects upon the child.

Nevertheless, all of these provisions of the GDPR regarding profiling have been criticized by the WP29 as being "shortened, unclear and restricted"[70], permitting video game companies to lawfully build children profiles, as long as the profile is built upon GDPR-compliant processing and if no automated decisions having legal or other significant effects on children is made. It has been argued[71] that this might represent a breach of children's online privacy and their right to development and to experiment with their own identity because of the lack of control they have over their personal data.

Children have the right to be properly informed about their rights under the GDPR, about the identity of the video game company or other entities processing their data with the occasion of playing a game, about the purpose, legal basis and the retention period of this data, about the contact details of the Data Protection Officer (DPO), as well as about their right to lodge a complaint in case of infringement[72]. For creating the framework for the actual implementation of these provisions, video game companies have the obligation to adopt privacy policies that are formulated "in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child,"[73] so that the child "can easily understand"[74] it. The actual implementation of these provisions is to be further determined by adopting codes of conduct[75], such as the UK's "The age-appropriate design: a code of practice for online services" which contains valuable guidelines. Although the UK is no longer a Member State of the EU, this Code can be referred to for improving the EU's normative framework in this area.

[66] Opinion 02/2013 (n 59).
[67] Article 29 Data Protection Working Party, 'Advice Paper on Essential Elements of a Definition and a Provision on Profiling within the EU General Data Protection Regulation' (2013).
[68] The European Data Protection Board 'Endorsement 1/2018 ' (2018).
[69] Recital 71 of the GDPR
[70] V Verdoodt, D Clifford and E Lievens, 'Toying with Children's Emotions, the New Game in Town? The Legality of Advergames in the EU' [2015] Privacy Law Scholars Conference, Proceedings.
[71] Lievens and Verdoodt (n 50).
[72] Art. 13 of the GDPR
[73] Art. 12 of the GDPR
[74] Recital 58 of the GDPR
[75] Lievens and Verdoodt (n 50).

Of course, children have all the rights granted to any other data subject, such as: right to withdraw the consent at any time, in an easily accessible manner[76], right of access the data that the video game company stores about them[77], right to data portability[78]. The latter is reflected in the obligation of the game company to provide a player with their personal data for transferring purposes to another game platform upon request. Another important right that children have is the right to erasure[79]. One application of this principle is erasing a child's MMORPG character out of the game without impacting the game environment.[80] Another hypothetical example that can be presented to illustrate this applicability is the participation of children in an MMORPG real-life competition (for example, a World of Warcraft tournament), having their personal data (their real name and their in-game character name) published on the official website. Later on in life, they might want this data to be removed as they no longer wish to be associated with the game they used to play as children. The possibility to have their data erased is affirmed to be in their best interest and to support their right to explore and experiment using their own identity, since the persistence and searchability of certain personal data online might impede this exploration.[81]

One challenge for video game companies is to justify the processing of biometric data and other data considered to be "sensitive", such as data concerning health, sexual life or sexual orientation, especially when the data subject is a child, as depicted in a previous chapter. Perhaps the most frightening aspect regarding the processing of biometric data is that most video game consoles continue to collect data even when the player is offline,[82] violating the right to privacy, not only in the online environment, but also in real life. Obviously, in this case, the manufacturers of these consoles do not comply with the above-stated principles namely the privacy-by-design principle, which would not have allowed the introduction of such a mechanism for continuous collection of biometric data, and the privacy-by-default principle, which would have implicitly stopped the collection of data posing the privacy of the user at high risk.

Besides the obligation to carry out a data protection impact assessment (DPIA), whenever the processing is performed using new technologies and is likely to result in a high risk to the rights and freedoms of the individuals[83], video game companies should implement additional safeguards when the data subject is considered "vulnerable", which is the case if the subject is a child.[84] Recital 91 of the GDPR recommends that such a DPIA to be carried out in case of processing biometric data, even if this would not result in a "high risk" for the privacy of the subject.[85]

[76] Art. 7 of the GDPR
[77] Art.15 of the GDPR
[78] Art. 20 of the GDPR
[79] Art. 17 of the GDPR
[80] Wessing, Hartlaub and Stach (n 42).
[81] Lievens and Verdoodt (n 50).
[82] Newman, Jerome and Hazard (n 28).
[83] Art. 35 of the GDPR
[84] Article 29 Data Protection Working Party, 'Opinion 03/2012 on Developments in Biometric Technologies' (2012)
[85] Recital 91 of the GDPR

To close the circle of special protection granted to children, the GDPR instates greater accountability on video game companies, which have to implement the appropriate technical and organisational measures to demonstrate that their processing is in compliance with the norms.[86] Additionally, supervisory authorities, while fulfilling their obligation of promoting public awareness and understanding of the "risks, rules, safeguards and rights"[87] regarding the processing of personal data, they have to devote special attention to children, designing special activities targeted at them in this regard.

To conclude this section, it is obvious that the GDPR aims to protect the best interests of the children, supporting their right to online privacy and data protection; however, there are still several obscure areas where is GDPR remains silent or creates legal uncertainty. Therefore, a possible efficient solution could be provided by alternative self-regulatory instruments. [88] Self-regulation represents a set of rules, entirely or partially designed, implemented and enforced by private stakeholders. This mechanism is considered to be more timely-efficient, flexible and adaptable to the rapid technological developments than the ordinary legislative procedure[89], as well as more efficient in mitigating the risks due to the increased level of expertise and collaboration between multiple stakeholders.[90]

4. Recommendations

As already mentioned, for an increased efficiency and a significant reach of these recommendations, a multi-stakeholder approach is recommended for creating a safer online environment for children, in the context of video games, from a data protection perspective.

4.1 Recommendations for video game providers

Video game providers should:

a) Comply with the principle of data minimization, not collect personal data of children unless this is strictly necessary for providing the service or optimizing it.[91] The smaller the amount of personal data, the smaller the risk for children's online privacy;
b) Approach cautiously any intention to use the children's personal data for purposes other than the provision of the service. The use of behavioural advertising aimed at children or profiling techniques are strongly discouraged, especially if this is contrary to the best interests of the child and are likely to influence and exploit the child's emotional vulnerability;
c) Carefully choose the legal basis for the processing. If consent is relied upon as a legal basis, either it be the child's or the parent's, as the case may be, the video game

[86] Article 24 of the GDPR
[87] Article 57 of the GDPR
[88] E Lievens, 'The Use of Alternative Regulatory Instruments to Protect Minors in the Digital Era: Applying Freedom of Expression Safeguards' (2011) 29 Netherlands Quarterly of Human Rights 164 <http://journals.sagepub.com/doi/10.1177/016934411102900202> accessed 4 March 2020.
[89] ibid.
[90] J de Haan and others, 'Self-Regulation' in E Staksrud, S McLaughlin B. O'Neill (eds), *Towards a better Internet for Children. Policy pillars, player and paradoxes*, vol 43 (1st edn, Nordicom (Goteborg) 2013).
[91] Lievens and Verdoodt (n 50).

provider should implement a verification mechanism as reliable as possible to verify the age of the minor or the existence and validity of the consent of the parent / legal guardian. If the game provider relies upon "legitimate interest" as a legal basis, the processing should be limited to the provision and improvement of the service. It should not be extended to the use of marketing techniques, given that the interests of the child easily prevail over the interests of the controller[92] (which is represented, in this case, by the game provider);

d) Comply with the principle of transparency set out in Article 12 of the GDPR, by drafting clear and concise privacy policies, formulated in plain language, in an unambiguous way, containing in particular information about: the types of data that are collected, the purposes of the processing, the rights of the user, as well as the exact measures that he can be taken in case a violation of these rights occurs. Video game providers can also create interactive and appealing privacy policies, perhaps by integrating game characters to briefly present the major points of interest before creating the account or before each authentication;
e) Comply with the principles of "privacy-by-design" and "privacy-by-default" by creating secure gaming tools, that fully respect the user's privacy, both online and offline, and ensure that game settings are set by default to provide a maximum level of privacy, without any further intervention from the user in order to deactivate options that could pose a risk to the minor's privacy;
f) Take steps to maintain an appropriate data security system to prevent minors' data, in particular sensitive and biometric data, from being accessed by unauthorized parties. In addition, the game provider should ensure appropriate training for its staff so that they are able to respect professional secrecy obligations regarding any personal data they come into contact with[93], and to react promptly in the event of a cyber-attack or a data breach;
g) Carry out a data protection impact assessment (DPIA)[94] before starting to process players' personal data, as the processing of children's personal data is considered to pose a high risk.[95] Moreover, an additional assessment must be performed whenever the processing involves the processing of biometric data, an assessment that can be integrated into the assessment of the impact on data protection under the GDPR.[96]

4.2 Recommendations for parents

It is undeniable that parents play a major role in their children's online experiences, significantly contributing to the protection of their online privacy and personal data, in the sense that the sole responsible and efficient intervention of a digitally-literate parent would be

[92] Verdoodt, Clifford and Lievens (n 71).
[93] Article 29 Data Protection Working Party, 'Advice Paper on Special Categories of Data ("sensitive Data")' (2011).
[94] Art. 35 of the GDPR
[95] Lievens and Verdoodt (n 50).
[96] Kindt Els, 'Biometric Applications and the Data Protection Legislation' [2007] Datenschutz und Datensicherheit 31 166 <http://www.fidis.net/fileadmin> accessed 8 March 2020.

sufficient for attaining these goals, without resorting to any other measures.[97] However, there are certain obstacles for reaching full parents' empowerment, either technical or social.
Therefore, parents should:

a) Treat with due diligence their supervisory duties, inform themselves and directly address to the video game provider any privacy concerns and queries related to their child, after carefully reading the game's privacy policy;
b) Make all efforts to have a productive dialogue with their children, to make informed decisions together regarding the online conduct of the child, relating to, for example, playing a certain game or not, purchasing game content, interacting with other players. However, it should be kept in mind that a total prohibition for the child to play video games might impede their right to play, interact and develop;[98]
c) Balance their supervisory duties with the children's right to privacy, which ought to be respected by parents themselves. If a parent monitors too closely the child's online activity, this might represent an infringement of the child's privacy.

4.3 Recommendations for children

Children themselves, together with their multiple rights that they are granted in the digital environment, should have certain responsibilities stemming from their online empowerment, according to their age and level of maturity.
Therefore, children should:

a) Inform their parents regarding the video games they play and ask for their authorisation/for their consent;
b) Change their account passwords often;
c) Not engage in interactions with other players, sharing personal information, either by the in-game chat, or through platforms outside of the game;
d) Nor perform any in-game payments without the approval of a parent;
e) Quickly inform a parent if they think that they have been the victim of a data breach (they can no longer access their account, their avatar has been stolen etc.) or of an in-game harrasement.

4.4 Recommendations for authorities

Of course, for protecting children's online rights, authorities involved in the policy-making process, both at an EU and a national level, together with the DPAs, play a major role. In this regard, they should take certain measures to ensure that children in the EU are properly informed about their data protection rights, how to exercise them and what to resort to in case of violation. This process can be achieved, on the one hand, via materials aimed directly at children, such as informational videos or even games. For example, the Joint Research Center of the European Commission launched a game, the "Cyber Chronix", which aims to inform

[97] Livingstone and O'Neill (n 33).
[98] ibid.

children about their rights under the GDPR.[99] On the other hand, informing children can be done indirectly, through a pedagogical approach, including teachers and school lessons, contributing to shaping the future digitally responsible citizens.[100]

At an EU level, the Research for CULT Committee outlines several recommendations.[101] First of all, they encourage research by European funding, oriented towards a deepened and multi-national understanding of the issues governing children as ”digital service users”, addressing their vulnerabilities, responsibilities and concerns, taking into account their level of perception, maturity and their background. Secondly, ”user empowerment and media literacy” of both parents and children is suggested, as a joint effort of the public and private sector. Thirdly, ”stakeholder coordination and cooperation” is highly encouraged, by actively involve children in this process, alongside with designers and lawyers[102] for simplifying the information.

To effectively exercise their data protection rights, children should be able to complain, in case of a violation, to anyone, such as parents or teachers, not only to the DPAs.[103] In this regard, parents and teachers require proper training, to be able to react promptly and take the necessary measures. Also, the DPAs should run awareness-raising campaigns, as part of their official duties.[104] Through these campaigns, they should encourage a common effort of video game industry, parents and governments in the sense of providing guidance to parents on how to engage with their children in their online activities and how to efficiently make use of the available parental control tools.

5. Conclusions

To conclude, the video game industry is increasingly providing its services to children, performing, at the same time, massive processing of their personal data. This paper has illustrated the situations when the processing of children’s personal data performed by video game companies should be regarded as “abusive”, by correlating different aspects of the gaming experience with the relevant provisions of the UNCRC and of the GDPR, two of the main legal instruments aiming to ensure that the best interests of the child are observed in every action undertaken by a video game provider.

[99] Joint Research Centre of the European Commission, ‘Cyber Chronix | EU Science Hub’ (2018) <https://ec.europa.eu/jrc/en/research-topic/security-privacy-and-data-protection/cyber-chronix> accessed 26 March 2020.
[100] J Persson‘CPDP 2020’ *Children’s privacy in the digital age* (2020) https://www.youtube.com/watch?v=2ss-Q88YHEE.
[101] S Livingstone, D Tambini and N Belakova, ‘Research for CULT Committee - Recommendations for EU Policy Developments on the Protection of Minors in the Digital Age ' European Parliament, Policy Department for Structural and Cohesion Policies (2018) <https://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_IDA%282018%29617454> accessed 4 March 2020.
[102] Lievens and Verdoodt (n 150).
[103] R Chatellier, ‘ CPDP 2020: Children’s Privacy in the Digital Age.’ (2020) <https://www.youtube.com/watch?v=2ss-Q88YHEE&t=433s> accessed 26 March 2020.
[104] Art. 57 of the GDPR

The purpose of this paper was to identify possible solutions for protecting children against this abusive personal data processing performed by video game providers, capable of violating their online privacy and data protection rights and exploiting their emotional vulnerability, lack of experience and critical thinking. This objective can be achieved through a multi-stakeholder approach, getting video game industry, parents, authorities and even children themselves collaborate towards ensuring an appropriate level of protection for children in the digital environment, while allowing them to benefit from the game experience, which might ensure the exercise of their rights under the UNCRC. Therefore, the challenge that arises for all of the above-mentioned stakeholders is balancing these two aspects. One the one hand, game providers should ensure a high level of privacy for children accessing their service, by being GDPR-compliant and by protecting their data from being wrongfully manipulated, while preserving their freedom of expression, right to play and to leisure activities, by adapting their service accordingly, rather than totally excluding children from accessing it. On the other hand, parents should balance their upbringing and monitoring duties with the child's right to privacy and to experiment using their own identity, by not being excessively strict or overly zealous in surveying the child.

In addition to this, on a legislative level, several improvements need to be considered, to ensure that the legislative framework is adapted to the rapid technological changes that occur in the gaming environment. It is undeniable that the online world increasingly resembles the offline world; therefore, the situations that arise within a virtual universe, especially when the player is a child, need to be rigorously regulated by enforceable acts and enforced by competent and, if possible, child rights-minded authorities. To be kept in mind that there is a "growing acceptance that what is illegal or inappropriate offline is or should be illegal or inappropriate online".[105]

Bibliography

I. Primary sources

International and regional legislation

UN General Assembly, 'Convention on the Rights of the Child',1989, United Nations, Treaty Series, vol. 1577, p. 3

EU legislation

- European Union, *Charter of Fundamental Rights of the European Union*, 2007, OJ C 303/2
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data [2016] OJ L119/1

[105] Livingstone and O'Neill (n 33).

- Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services [2015] *OJ L 241*

II. Secondary sources

Books and book chapters

- Comas J , Tschang F, 'The Brief History, Tumultuous Present and Uncertain Future of Virtual Worlds (Terrae Fabricatae)' in S Hotho, N McGregor (eds) *Changing the Rules of the Game: Economic, Management and Emerging Issues in the Computer Games Industry* (Palgrave Macmillan 2013).
- De Haan J and others, 'Self-Regulation' in E Staksrud, S McLaughlin B. O'Neill (eds), *Towards a better Internet for Children. Policy pillars, player and paradoxes*, vol 43 (1st edn, Nordicom (Goteborg) 2013).
- Livingstone S , O'Neill B, 'Children's Rights Online: Challenges, Dilemmas and Emerging Directions' Children' in S van der Hof, Van den Berg B, Schermer B (eds) *Minding Minors Wandering the Web: Regulating Online Child Safety* (Springer 2014).
- Newman J, Simons I and Jarvis E, *Difficult Questions about Video Games* (Suppose Partners 2004).
- Van der Hof S, 'No Child's Play: Online Data Protection for Children' in S van der Hof, Van den Berg B, Schermer B (eds) *Minding Minors Wandering the Web: Regulating Online Child Safety* (Springer 2014).

Articles

- Badrinarayanan V, Sierra J and Martin K, 'A Dual Identification Framework of Online Multiplayer Video Games: The Case of Massively Multiplayer Online Role Playing Games (MMORPGs)' [2015] 68 Journal of Business Research 1045
- Bygrave L, 'Data Protection by Design and by Default : Deciphering the EU's Legislative Requirements' (2017) 1 Oslo Law Review 105.
- Holloway D, 'Surveillance Capitalism and Children's Data: The Internet of Toys and Things for Children' (2019) 170 Media International Australia 27 <http://journals.sagepub.com/doi/10.1177/1329878X19828205> accessed 4 March 2020
- Kindt E, 'Biometric Applications and the Data Protection Legislation' [2007] Datenschutz und Datensicherheit 31 166 <http://www.fidis.net/fileadmin> accessed 8 March 2020.
- Lievens E, 'The Use of Alternative Regulatory Instruments to Protect Minors in the Digital Era: Applying Freedom of Expression Safeguards' (2011) 29 Netherlands Quarterly of Human Rights 164 <http://journals.sagepub.com/doi/10.1177/016934411102900202> accessed 4 March 2020.
- Lievens E, Verdoodt V, 'Looking for Needles in a Haystack: Key Issues Affecting Children's Rights in the General Data Protection Regulation' (2018) 34 Computer

Law & Security Review 269 <https://linkinghub.elsevier.com/retrieve/pii/S026736491730314X> accessed 4 March 2020.

- Lupton D and Williamson B, 'The Datafied Child: The Dataveillance of Children and Implications for Their Rights' (2017) New Media & Society, 19(5) 780-794 <https://doi.org/10.1177/1461444816686328> accessed 14 February 2020.
- Newman J, Jerome J and Hazard C, 'Press Start to Track? Privacy and the New Questions Posed by Modern Videogame Technology' [2014] American Intellectual Property Law Association (AILPA) Quarterly Journal 1.
- Nielsen D, 'Identity Performance in Roleplaying Games' (2015) 38 Computers and Composition 45
- Schafer B and Abel W, 'All the World's a Stage — Legal and Cultural Reflections on the Surveillance of Online Games' (2014) 38 Datenschutz und Datensicherheit - DuD 593-600

Other secondary sources

- Article 29 Data Protection Working Party, 'Advice Paper on Special Categories of Data' (2011).
- Article 29 Data Protection Working Party, 'Opinion 03/2012 on Developments in Biometric Technologies' (2012)
- Article 29 Data Protection Working Party, 'Opinion 02/2013 on Apps on Smart Devices' [2013]
- Article 29 Data Protection Working Party, 'Advice Paper on Essential Elements of a Definition and a Provision on Profiling within the EU General Data Protection Regulation' [2013]
- The European Data Protection Board 'Endorsement 1/2018 ' [2018].
- Information Commissioner's Office, 'Age-Appropriate Design Code: a code of practice for online services' (2020).
- Joint Research Centre of the European Commission, 'Cyber Chronix | EU Science Hub' (2018) <https://ec.europa.eu/jrc/en/research-topic/security-privacy-and-data-protection/cyber-chronix> accessed 26 March 2020.
- Livingstone S, Tambini D, Belakova N, 'Research for CULT Committee - Recommendations for EU Policy Developments on the Protection of Minors in the Digital Age' European Parliament, Policy Department for Structural and Cohesion Policies (2018) <https://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_IDA%282018%29617454> accessed 4 March 2020
- Verdoodt V, Clifford D and Lievens E, 'Toying with Children's Emotions, the New Game in Town? The Legality of Advergames in the EU' [2015] Privacy Law Scholars Conference, Proceedings.
- Recital 38 of the GDPR
- Recital 47 of the GDPR
- Recital 58 of the GDPR

- Recital 60 of the GDPR
- Recital 71 of the GDPR
- Recital 91 of the GDPR
- Recial 135 of the GDPR

III. Websites and blogs

- Bänsch J, 'CPDP 2020', *Children's privacy in the digital age* (2020) https://www.youtube.com/watch?v=2ss-Q88YHEE accessed 26 March 2020.
- Blickensderfer S and Brown N A, 'S1:E3 - Even the Games Have Eyes: Data Privacy and Gaming | Carlton Fields' (2019) <https://www.carltonfields.com/insights/podcasts/lan-party-lawyers/games-have-eyes-data-privacy-gaming> accessed 4 March 2020
- Chatellier R, ' CPDP 2020: Children's Privacy in the Digital Age.' (2020) <https://www.youtube.com/watch?v=2ss-Q88YHEE&t=433s> accessed 26 March 2020.