



Annales de la Faculté de Droit d'Istanbul

RESEARCH ARTICLE / ARAŞTIRMA MAKALESİ

Privacy Screening of Online Game Platforms: A Case Study of “Gamecell”

Çevrim içi Oyun Platformlarının Gizlilik Taraması: “Gamecell” Analizi

Leyla Keser Berber¹ , Ayça Atabey² 

Abstract

Online games and the usage of the Internet are now ubiquitous in the lives of children. From widespread engagement with the Internet through ever changing technologies, children and parents are now faced with a plethora of risks for which they need protection. Despite strong legal instruments in most countries on data protection and privacy, there is still a need to see child privacy on the ground. To that extent, this paper looks into Gamecell - a popular online game platform - by addressing “accountability” of the platforms based on their data protection and privacy obligations under the relevant laws and draw attention to the company’s current practices, aiming to show the gaps existing between theory and practice. By urging all the stakeholders of the online gaming ecosystem to take the necessary steps for accountability reasons, and to truly understand the rules set out in the applicable legal framework, we argue that users’ rights and freedoms are non-negotiable. Finally, we emphasize that stakeholders of the online gaming ecosystem should acquire a true understanding of the importance of “fairness” and online gaming companies should remember that it should be central to all your processing of children’s personal data.

Keywords

Online gaming, privacy, children’s rights, data protection, accountability

Öz

Çevrim içi oyunlar çocukların hayatında önemli bir yere sahiptir. Çocuklar, yaygın internet kullanımı ve sürekli değişen teknolojilerin yarattığı riskler nedeniyle korunmaya ihtiyaç duymaktadır. Birçok ülkede mahremiyet ve veri koruması ile ilgili güçlü yasalar olmasına rağmen, çocuk mahremiyeti konusunda yeterli hassasiyet gösterilmemektedir. Bu makale, bilinen bir çevrim içi oyun platformu olan Gamecell’in uygulamalarını ilgili yasalar ile düzenlenen “hesap verilebilirlik” ilkesi kapsamında incelemekte ve uygulamadaki aksaklıklara dikkat çekmektedir. Bu makale, aynı zamanda, çevrim içi oyun ekosisteminin tüm paydaşlarının hesap verebilirlik ilkesini özümsemeye teşvik etmeyi ve kullanıcılara karşı yükümlülüklerini hatırlatmayı amaçlamaktadır. Son olarak, çevrim içi oyun ekosisteminde yer alan tüm paydaşların veri işleme faaliyetleri kapsamında dürüstlük ilkesini içselleştirmeleri gerektiği savunulmaktadır.

Anahtar Kelimeler

Çevrim içi oyunlar, mahremiyet, çocuk hakları, kişisel verilerin korunması, hesap verilebilirlik

1 **Corresponding Author:** Leyla Keser Berber (Prof.), Istanbul Bilgi University, Faculty of Law, Information Technology Law Institute, Istanbul, Turkey. E-mail: leyla.keser@bilgi.edu.tr ORCID: 0000-0002-2438-768X

2 Ayça Atabey (Researcher/ PhD student), Istanbul Bilgi University, Faculty of Law, Information Technology Law Institute, Istanbul, Turkey/ Edinburgh University, Law School, Edinburgh, UK. E-mail: ayca.atabey@ed.ac.uk ORCID: 0000-0003-3165-6750

To cite this article: Keser Berber L, Atabey A, “Privacy Screening of Online Game Platforms: A Case Study of “Gamecell””, (2020) 69 Annales de la Faculté de Droit d'Istanbul 181. <https://doi.org/10.26650/annaes.2020.69.0007>



Privacy Screening of Online Game Platforms: A Case Study of “Gamecell”

Introduction

Online games and the usage of the Internet are now ubiquitous and deeply ingrained in the lives of children. It is therefore imperative that stakeholders of the online gaming ecosystem to acquire a detailed understanding of the importance of children’s online privacy and the challenges that are relevant in today’s digital age in order to take necessary measures to protect children and respect their rights to privacy and data protection - two fundamental and in most countries such as Turkey, even recognized as a constitutional right under national law. Being one of the more vulnerable groups of society, children deserve more protection concerning their personal data. Luckily, there is an increasing awareness about personal data protection of children around the world. For instance, Apple and Google already conduct *privacy screening* for all apps, including games wanting to be on the Appstore and/or Google Play. Website versions of popular games pop up with cookie management tools and updated privacy policies in line with General Data Protection Regulation (“GDPR”) and/or other national data protection laws and regulations. Despite strong legal instruments in most countries on data protection and privacy and also positive measures taken in the sector, there is still a need to see child privacy on the ground. To that extent, we chose Gamecell - a popular online game platform, which bring game developers together with children as “users”. In this article, we will address the “*accountability*” of the platforms based on their data protection and privacy obligations under the relevant laws and draw attention to these companies’ current practices, aiming to show the gaps existing between theory and practice. “*Accountability*” means for the data controller to be responsible for and be able to demonstrate compliance with the core principles relating to the processing of personal data Article 5(2) under the GDPR. Accordingly, in order to assess Gamecell’s compliance with the accountability principle, we will first analyse the game platform by referring to the core principles set out under Article 5(1) of the GDPR with a focus on “*lawfulness, fairness and transparency*” principle, which is strongly linked with the notion of “*consent*”. However, as all the principles are interlinked in some way, there will be references to other principles and rules set out under the current data protection regime where necessary. This article underscores the fact that the core principles do complement each other and have a great role in exercising other rules laid out under the GDPR and the Turkish Data Protection Law (“KVKK”) as well. In order to assess companies’ compliance with the respective laws, this article looks into User Agreement, Terms of Service, Data Privacy Notice (Services), and Cookie and Privacy Policies of the two respective companies. Accordingly, our analysis findings and outcomes show us that there are still crucial problems in practice regarding compliance with personal data processing principles of related data protection laws and regulations, namely, the GDPR and

the KVKK. This article starts by setting the stage before it moves to the privacy screening of Gamecell. In Section II, company's relevant agreements and policies will be assessed to point out the gaps between the expectations arising from the rules set out under data protection regime and the implementation of these rules in practice. Through identifying the existing gaps, we will see whether Gamecell undermine children's rights pursuant to the rules under the GDPR and the KVKK. Lastly, in Section III, we refer to some recent developments and give practical examples from around the world in order to shed light on the steps which online gaming platforms could adopt for protecting children's rights and in the same time comply with the requirements prescribed by law. This article concludes that despite the recent developments in the internet governance ecosystem, online gaming companies are yet to take solid steps and make tangible changes in their terms and policies in order to achieve the purposes of the data protection regimes. In addition, we urge Gamecell as well as other companies to embrace the notion of 'fairness' and make it their prerequisite for every single step or any decision they may take, particularly if, such actions somehow involve or have a possibility to involve children.

I. Setting the Stage for Privacy Screening: Personal Data Protection and Children

This Section underscores the fact that children merit additional protection and draws attention to their vulnerable place in the society. It then briefly explains the legal framework relevant in this context in order to set the scene and provide an understanding of what the law requires before moving on to the privacy screening of Gamecell. Also, opinions of relevant authorities will be referred to before we delve into the companies' terms and policies.

Importance of Personal Data Protection for Children

It is a widely accepted fact that children should be treated differently than adults in many contexts. For instance, even in the countries where there is no comprehensive law on data protection, there are still rules and laws which protect children in terms of privacy under other laws.¹ This, in itself, shows how universal children's vulnerability and special position are recognised in different societies around the globe even in certain situations, comprehensive data protection laws do not exist. It is no brainer that children need additional protection when a company processes their personal data. This is because, as they form a vulnerable group of the society, they are less likely to be as aware of the risks involved as an adult would with relation to the processing carried out on their personal data. Accordingly, Recital 75 of the GDPR underscores

¹ 'The Keys to Data Protection A Guide for Policy Engagement on Data Protection' (2018) <[https://privacyinternational.org/sites/default/files/2018-09/Data Protection COMPLETE.pdf](https://privacyinternational.org/sites/default/files/2018-09/Data%20Protection%20COMPLETE.pdf)> accessed 24 February 2020.

that children are *vulnerable natural persons* and that processing activities involving children's data may result in risk of varying likelihood and severity. Accordingly, when online game platforms process children's personal data, the expectations are higher; these expectations require companies to think about the need to protect children from the outset, and design company's systems and processes with this in mind.² It is vital to understand how strong online games' impact can be on children to the extent that their health, lives, social relationships, academic success as well as mental disabilities' severity can be dramatically affected.³ When the processing carried out somehow relates to children, as arguably the most vulnerable group of the society, many rules and principles including the legitimate interests under the GDPR, they become more complex than ever, even when compared to other challenging situations such as processing special categories of data or when the public sector is involved. Similarly, children's data are usually considered to constitute a special category of data as such data require additional care.⁴ Speaking of vulnerability, it is noteworthy to state that although all children are vulnerable, some can be more vulnerable than others. Children coming from disadvantaged backgrounds, children with mental health issues, learning disabilities, psychological problems, children who are in a difficult position in their lives and possibly being neglected by their parents can be easily affected by the online gaming industry as much as advertising industry triggering internet addiction or other relevant risks in the internet ecosystem. Although it is not directly relevant in the context of this article, in order to show how much online video games can affect children, and how their design can be crucial, it is important to mention that videogames can even be used by people with malicious intentions who design online video games in order to convince and recruit children for unlawful purposes.⁵ The fact that the offenders choose online videogames as a tool is significant since it both shows the vulnerability of children and the impact online games may have on children. Recognising the universality of the risks attached to online games under the umbrella of general terms such as "online threats" or "privacy threats" would help all the stakeholders in the ecosystem to address different types of threats and differentiate harms that stem more from data exploitation, consumer identity and online presence of children in cases such as internet addiction problems and risks attached to exploitation of children's data to be used for online behavioural advertising. As children can be particularly susceptible in the online environment and more easily affected by behavioural advertising⁶, online

2 Information Commissioners Office, 'How Does the Right to Be Informed Apply to Children?' (2018) <<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr/how-does-the-right-to-be-informed-apply-to-children/>> accessed 18 February 2020.

3 See for example, Healthline, 'What Science Says About Video Games and ADHD' <<https://www.healthline.com/health-news/the-link-between-adhd-and-video-games>> accessed 24 February 2020.

4 *ibid.*

5 See for example UNODC, 'The Use of Internet for Terrorist Purposes' (2012).

6 See ICO, 'The General Data Protection Regulation Children and the GDPR' (2018) <<https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr-1-0.pdf>> accessed 24 February 2020.

gaming companies should demonstrate that they took additional steps to ensure that their priority is children's best interests. These, overall, are the pieces which should be taken into account to achieve the main objective of ensuring online child protection and ultimately enhancing their fundamental rights and freedoms. While a multitude of opportunities arise from the digital environment, so too can the potential for increased exposure to risks such as exposure to age-inappropriate advertising and data misuse.⁷ These risks can affect children's well-being and undermine their right to privacy. Overall, it is a fact that with the current speed at which technology is evolving, it is impossible to accurately predict what is to come. Use of online gaming platforms and rapidly changing technologies are more involved in children's lives now more than ever. Protecting children - vulnerable members of the society, the future of tomorrow's society - against online abuse, exploitation of their data or undermining their fundamental rights and freedoms should be prevented and protecting them online should be one of the key goals of not only nations but also the international community and society.

Legal Framework: GDPR and KVKK

After summarising the relevance of children's vulnerability in the online ecosystem in general and online game industry in particular, this subsection delves into the legal framework relating to data protection regimes in question. The GDPR provides specific rules with regards to processing children's data⁸. Although the encompassing term of 'vulnerable' is used in relevant provisions, the main focus remains to be on children under the data protection regime. This vulnerable nature of children is highly interlinked with the application of the rules set out under the data protection regime and their close intersection with the notion of 'fairness'. Accordingly, it is noteworthy to state that the concept of fairness is of utmost importance when carrying out activities involving children's personal data processing despite the fact that compliance with all the core principles and rules is still required under the GDPR. Regarding children's protection, one of the most relevant provisions under the GDPR is Article 6(1), which lays out conditions that determine the "Lawfulness of processing". Article 6(1) is highly interlinked with Article 5(1)(a) of the GDPR. A processing activity can be considered as lawful only if and to the extent that at least one of the conditions provided under Article 6(1) apply. Thus, in order to carry out processing involving children's personal data, there is a need to have and justify a lawful basis under the GDPR. Consent is one possible lawful basis for processing, however as the Information Commissioner's Office ("ICO") notes down, there are

7 See for example Kate Raynes-Goldie and Matthew Allen, 'Gaming Privacy: A Canadian Case Study of a Co-Created Privacy Literacy Game for Children' <<http://pdfs.semanticscholar.org/1e30/e92594e9728148b5438be71e51943d0ae9c4.pdf>> accessed 24 February 2020.

8 Please note that the term "child" is not defined by the GDPR; therefore, online gaming companies should take an inclusive approach and take into account the needs of teenagers and young people who are below 18, but also young adults; See page 2 Bird&Bird, 'Principles | Children' <<https://www.twobirds.com/~media/pdfs/gdpr-pdfs/24--guide-to-the-gdpr--children.pdf?la=en>> accessed 24 February 2020. Raynes-Goldie and Allen (n 7).

alternative⁹ grounds constituting a lawful basis for processing. According to the ICO, using other options different than ‘consent’ can occasionally be more appropriate and offer better protection for children.¹⁰ However, it is also crucial to note that reliance on an alternative option should not be abused. The June 2019 Report of the European Commission Multi-stakeholder Expert Group on the GDPR application states that there are concerns about allowing digital platforms to choose other legal bases than depending on the national legislation in the respective Member States.¹¹ This is especially the case for choosing the contract legal basis under Article 6(1) (b) depending on the age of children for entering into a contract applicable in the respective national laws.¹² The Report highlights warnings of the consumers’ organisations working with children’s welfare organisations, urging online platforms to be careful and not to abuse the system.¹³ They advise that such practices circumvent the obligations under Article 8 and can lead to a fragmentation among Member States and therefore will contradict with the objectives of the GDPR.¹⁴ If consent is chosen over its alternatives, when offering an online service directly to a child, the online gaming company, which operates and provides services in different Member States in the EU (e.g.: Gamecell), is expected to take the minimum age for being able to give consent under the respective jurisdiction to achieve the purposes of the data protection regime. This is because although the GDPR provides parental consent requirement for children under 16 in situations where information society services are offered directly to them, Member States are allowed to opt to depart from and choose to lower this age threshold to 15, 14, or 13 years - cannot be below 13.¹⁵ This flexibility provided to Member States has caused complexities in practice and created confusion among stakeholders of the online ecosystem including parents.¹⁶

9 See ‘Contribution from the Multistakeholder Expert Group to the Stock-Taking Exercise of June 2019 on One Year of the GDPR Application’ (2019) <<http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupId=3537&NewSearch>> accessed 24 February 2020. Page 10

10 ‘Children | ICO’ <<https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/children/>> accessed 24 February 2020.

11 ‘Contribution from the Multistakeholder Expert Group to the Stock-Taking Exercise of June 2019 on One Year of the GDPR Application’ (n 9).

12 *ibid.* See also ‘GDPR Implementation In Respect of Children’s Data and Consent Centre for Information Policy Leadership 6 March 2018 2 CIPL’s TOP TEN MESSAGES ON GDPR IMPLEMENTATION IN RESPECT OF CHILDREN’S DATA’ (2018) <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_-_gdpr_implementation_in_respect_of_childrens_data_and_consent.pdf> accessed 24 February 2020.

13 *ibid.*

14 *ibid.*

15 Article 8 “(1) Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years; (2) The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology; (3) Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.”

16 See ‘Contribution from the Multistakeholder Expert Group to the Stock-Taking Exercise of June 2019 on One Year of the GDPR Application’ (n 9). Page 10; See also Ingrida Milkaitė and Eva Lievens, ‘Better Internet for Kids - Status Quo Regarding the Child’s Article 8 GDPR Age of Consent for Data Processing across the EU’ (2019) <<https://www.betterinternetforkids.eu/web/porta/practice/awareness/detail?articleId=3017751>> accessed 18 February 2020.

There are many criticisms on the Article 8's age threshold, which is understandable. This is because having different age limits in different countries is not necessarily meaningful in the sense that children's capacity cannot change from country to country.¹⁷ For example, in the UK only children aged 13 or over are able to provide their own consent. On the other hand, in France the age of consent is 15, while in Ireland and Germany the age of consent is 16. The reasoning behind these differences are yet to be understood and unsurprisingly draws much criticism.¹⁸ Accordingly, in practice, if a company wants to rely on consent, in addition to the GDPR, it should also check the national laws in which it operates.¹⁹ The need to make an extra effort to check the consent requirements of the country in which a company operates requires additional efforts and such differences may be challenging and even perplexing for different stakeholders of the ecosystem for practical reasons.

Another debated point in the GDPR involves the rules set out for profiling children and how decisions are to be made with respect to the legal basis for processing such as when the processing should be grounded on consent. Here, it is also crucial to point out that if a company considers profiling children for marketing purposes then there is a need to take into account the Article 29 Data Protection Working Party's comments in its Guidelines on Automated Individual decision-making and Profiling for the purposes of Regulation 2016/679.²⁰ Going back to consent, as Macenaite and Kosta point out, the GDPR is based on the premise that children can be protected through informed parental consent.²¹ Accordingly, other contentious questions arise: how parental consent is to be verified, and when and how risk-based impact assessments should be carried out?²² Article 8(2) requires the controller to make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology. Therefore, online gaming companies are expected to show that they make an effort to make sure that the person giving consent can give such consent for the purposes of Article 8, of course to the best possible extent, as much as the available technologies

17 See for example Sonia Livingstone, 'Children: A Special Case for Privacy? Article (Published Version) (Refereed)' (2018) <http://eprints.lse.ac.uk/89706/1/Livingstone_Children-a-special-case-for-privacy_Published.pdf> accessed 24 February 2020. Page 20

18 See Ingrida Milkaite and Eva Lievens (n 16).

19 See EDPB, 'Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3)-Version for Public Consultation' (2018) <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_en.pdf> accessed 24 February 2020. Page 12 "*Controllers and processors must therefore ensure that they are aware of, and comply with, these additional conditions and frameworks which may vary from one Member State to the other. Such variations in the data protection provisions applicable in each Member State are particularly notable in relation to the provisions of Article 8 (providing that the age at which children may give valid consent in relation to the processing of their data by information society services may vary between 13 and 16)...*"

20 See Article29, 'ARTICLE29 Newsroom - Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679 (Wp251rev.01) - European Commission' (2018) <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053> accessed 24 February 2020.

21 Milda Macenaite and Eleni Kosta, 'Consent for Processing Children's Personal Data in the EU: Following in US Footsteps?' (2017) 26 Information and Communications Technology Law 146.

22 *ibid.*

allow. It is also noteworthy to state that if online game platforms rely on consent, they are expected to ensure that children comprehend what they are consenting to and understand the rights they have including ‘right to access’²³. Informing children about their rights would also help children appreciate or at least trigger them to think about the importance of ‘consent’. Such a practice would also give them an idea about their place in this online world, making them understand that they are being recognised as separate individuals who have their rights, and not merely users behind the screen, who are been taken granted for. This is important for transparency and fairness elements both under the GDPR and the KVKK. Similarly, it is crucial to note that consent could provide “illusionary control”²⁴ in many ways, not only for children but also for parents. Thereby, the doors become more open to abuse and exploitation that results from the imbalance of power between data subjects (both children and adults) and online gaming companies. In addition to providing unambiguous information to children, it is also important that the companies make sure that parents also understand the implications and effects of what they are consenting to. As Article 29 Data Protection Working Party confirms, in the context of such a power imbalance, the agreement to the processing of personal data cannot be considered to be delivered freely.²⁵ To elaborate, in circumstances where consent is ‘bundled up’ as a non-negotiable part of terms and conditions in a contract, it would fail to constitute a valid consent for the purposes of the GDPR. This is because the consent that is bundled up as a non-negotiable part of a contract is presumed not to have been freely given.²⁶ Therefore, online gaming companies’ genuine efforts in ensuring that they obtain consent in a fair manner is critical.

Coming back to Article 5(1)(a) GDPR, which provides that personal data must be processed lawfully, fairly and transparently in relation to the data subject, this core principle of fairness includes taking into account the reasonable expectations of the data subjects,²⁷ bearing in mind possible adverse consequences data processing can have on data subjects, and having regard to the relationship and potential effects of imbalance between them and the controller. Although there is an imbalance between adults and online gaming companies as well, this imbalance and the effect it has on data subjects increase when the data subject is from a vulnerable group of the

23 See ‘Right of Access | ICO’ <<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/>> accessed 24 February 2020. Note that “*Even if a child is too young to understand the implications of subject access rights, it is still the right of the child rather than of anyone else such as a parent or guardian.*”

24 Laura Brandimarte, Alessandro Acquisti and George Loewenstein, ‘Misplaced Confidences’ (2013) 4 *Social Psychological and Personality Science* 340 <<http://journals.sagepub.com/doi/10.1177/1948550612455931>> accessed 24 February 2020.

25 See, for example, Macenaite and Kosta (n 21).

26 *ibid.*

27 Some personal data are expected to be private or only processed in certain ways, and data processing should not be surprising to the data subject. The concept of ‘reasonable expectations’ is specifically referenced in recitals 47 and 50 in relation to Article 6(1)(f) and (4) under the GDPR.

society, such as children.²⁸ Therefore, in our context, the imbalance between the data subjects (children) and the online platform (Gamecell) is imperative for the purposes of ensuring a correct reflection of the notion of 'fairness' in practice.

As a matter of lawfulness, contracts for online services must be valid under the applicable contract law.²⁹ An example of a relevant factor is whether the data subject is a child, for reasons such as capacity to enter into contractual relations. In such a case (in addition to ensuring compliance with the requirements prescribed by the GDPR including the 'specific protections' available to children, under Recital 38, children merit specific protection with regard to their personal data as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data), the controller must make sure that its practices are compliant with the relevant national laws on these capacity of children to enter into contracts.³⁰ Moreover, in order to make sure that the reasonable efforts are made for the purposes of Article 5(1)(a), online gaming companies are expected to satisfy other legal requirements under relevant laws and regulations. Looking from a contract law perspective, for instance, for consumer contracts, Directive 93/13/EEC on unfair terms in consumer contracts ("the Unfair Contract Terms Directive") is highly relevant.³¹ This is because a term which has not been separately negotiated on its own, cannot be considered as 'fair' for the purposes of the Unfair Contract Terms Directive.³² Also, Article 12(1) of the GDPR complements Article 5(1)(a) by providing that the information provided must be concise, transparent, intelligible and easily accessible. With regard to transparency, Article 29 Data Protection Working Party's approach is that "transparency is a free-standing right which applies as much to children as it does to adults".³³ In its report, the Article 29 Data Protection Working Party underscores specifically that obtaining consent by the holder of parental responsibility in a situation that falls under Article 8, does not mean that children can no longer use their rights as data subjects to transparency. This means that online gaming companies cannot hide behind the excuse of 'parental consent' for not making children friendly information available to inform children in a plain language.³⁴ In other words,

28 See also page 32 ICO, 'The General Data Protection Regulation Children and the GDPR' (n 6).

29 See EDPB, 'Guidelines 2/2019 on the Processing of Personal Data under Article 6(1)(b) GDPR in the Context of the Provision of Online Services to Data Subjects Adopted-Version for Public Consultation' (2019) <https://edpb.europa.eu/sites/edpb/files/consultation/edpb_draft_guidelines-art_6-1-b-final_public_consultation_version_en.pdf> accessed 24 February 2020. Page 5

30 *ibid.* See also 'ISFE Response to the ICO Public Consultation On Children and the GDPR' (2018) <www.isfe.eu> accessed 24 February 2020.

31 *ibid.*

32 *ibid.*

33 Article29, 'ARTICLE29 Newsroom - Guidelines on Transparency under Regulation 2016/679 (Wp260rev.01) - European Commission' <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227> accessed 24 February 2020. page 10

34 See also Natali Helberger, Frederik Zuiderveen Borgesius and Agustin Reyna, 'THE PERFECT MATCH? A CLOSER LOOK AT THE RELATIONSHIP BETWEEN EU CONSUMER LAW AND DATA PROTECTION LAW' (2017) 54 Common Market Law Review <https://www.ivir.nl/publicaties/download/CMLR_2017.pdf> accessed 24 February 2020. Article29 (n 33).

'parental consent' cannot be used as an excuse for prioritising adults, discriminating against children, and assume that they are not required to make additional efforts to be equally transparent to children. Furthermore, making sure that children can enjoy their right to transparency during "the continuum of their engagement"³⁵ with online gaming companies is also aligned with the Article 13 of the UN Convention on the Rights of the Child.³⁶ Similar to the transparency obligation in the GDPR, the Unfair Contract Terms Directive requires using unambiguous, clear and intelligible language.³⁷ Therefore, it can be concluded that an unfair processing of personal data that fails to comply with the notions of fairness, lawfulness, and transparency, would most probably also be regarded as an unfair term under the Unfair Contract Terms Directive.³⁸ In practice, even if the company relies on parental consent, as the Article 29 Data Protection Working Party clarified in its Transparency Report, children are still expected to be provided with information delivered in clear and plain language.³⁹ Accordingly, in order to comply with the specific mentions of transparency measures addressed to children in Article 12(1) (also supported by Recitals 38 and 58)⁴⁰, online gaming companies should make sure that if they target children or they know that children use their products or services, "*any information and communication should be conveyed in clear and plain language or in a medium that children can easily understand*".⁴¹ Therefore, it can be concluded that under the GDPR, children and adults are clearly separated with regards to the additional care expected to be taken when processing their personal data. On the other hand, unlike the GDPR, there is no specific provision(s) on children in the KVKK. However, according to Article 10 of the Turkish Constitution; "*everyone is equal before the law without distinction as to language, race, colour, sex, political opinion, philosophical belief, religion and sect, or any such grounds*". This means there is no distinction between adults or children in terms of having and using fundamental rights including rights to privacy and data protection. Similar to other countries, the age of consent is one of the important discussion topics in Turkey as well. KVKK has no clear guidance on that question. However, Turkish Civil Law answers that important question. Legal capacity is assessed on the criteria of mental competence, maturity and non-restriction in Turkish law. It will be appropriate to consider the legal capacity of non-mature individuals

35 Article29 (n 33).

36 Article 13 of the UN Convention on the Rights of the Child states that: "*The child shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of the child's choice.*"

37 See 'European E-Justice Portal - Unfair Contract Terms Directive (93/13)' <https://e-justice.europa.eu/content_unfair_contract_terms_directive_9313-627-en.do> accessed 24 February 2020.

38 See also EDPB (n 29). Page 5

39 See Article29 (n 33).

40 Note that Recital 58 explicitly states as follows and emphasizes that the language used should be clear for children to understand "*Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand.*"

41 Article29 (n 33). Page 11

– children according to their lack of mental competence. However, it should not be forgotten that the concept of mental competence is a relative concept and should be evaluated separately for each separate act in law.

Children who are not mentally competent are considered to fully lack legal competence (they are regarded as fully incompetent) and all of their acts are carried out by their legal representatives (TMK Article 15). Children who are mentally competent are considered as partially incompetent (TMK Article 16/I). As a rule, partially incompetent children, carry out their actions in law with the permission or consent of their legal representative (parent-guardian). Exceptionally gifts and the use of strictly dependent rights do not require the permission or approval of the legal representative. In terms of the aforementioned act in law, children can exercise their rights and can incur liabilities only with their own actions. Therefore, the point to be discussed is whether the right to consent to the processing of personal data is strictly dependent on an individual. Since personal data constitutes one of the personality values that form a part of the personality rights under Turkish law, free from doctrinal debates, we believe that the consent activity for the processing of personal data should also be regarded as the exercise of a right strictly dependent on an individual. This is because the activities of showing consent to the attacks against other personality values in accordance with the law are also defined as the strict use of rights in the doctrine.

Overall, it is clear children are expected to be treated with additional care to ensure that their rights are protected effectively. To do this, first all stakeholders should acquire a detailed understanding of the law relevant in this context. The above discussions provide a summary of the most relevant rules that are prescribed by law, which do not seem to be thoroughly understood as we will emphasize in detail in Section II. After setting the scene from a legal perspective, the next subsection will support the importance of putting the law into practice and making sure that all stakeholders understand the place of online games in children's lives.

Children and Online Gaming Industry

The online gaming industry is one of the fastest growing entertainment industries in the world.⁴² Digital games are up three percent year over year having generated \$120.1 billion in 2019 and increased by an \$11 billion compared to last year.⁴³ It is a widely accepted fact that the booming online gaming industry is deeply ingrained

42 Amaya Gorostiaga and others, 'Child Rights and Online Gaming: Opportunities & Challenges for Children and the Industry' (2019) <https://www.unicef-irc.org/files/upload/documents/UNICEF_CRBDigitalWorldSeriesOnline_Gaming.pdf> accessed 18 February 2020.

43 See '2019 Year In Review — SuperData, a Nielsen Company' <<https://www.superdataresearch.com/2019-year-in-review>> accessed 24 February 2020.

in the lives of children with the ubiquitous and rapidly changing technologies.⁴⁴ It is therefore crucial that all the necessary steps and reasonable measures to be taken as soon as possible without causing any more delay or infringement of children's rights to data protection and privacy in the online gaming ecosystem. In order to do this, the extent to which the online gaming industry can have an effect on children's and parents' lives should be appreciated. Although there may be benefits⁴⁵ to include children in the online gaming ecosystem, it can also have negative effects on children's lives.⁴⁶ An EU study on the impact of marketing through online services including online games and mobile applications on children's behaviour found that advertising have clear and sometimes subliminal effects on children's behaviour.⁴⁷ There are many examples showing how children can be affected negatively from online games, where children's rights can be undermined.⁴⁸ One of the examples where the vulnerable nature of children becomes highly relevant in the online gaming ecosystem concerns the processing activities carried out for profiling purposes. This is because profiling can be used to target data subjects that the algorithm considers are more likely to spend money on the services provided or to deliver more personalised ads. The age and maturity of the child may affect their ability to comprehend the reason and purpose behind the ads shown or the consequences of the data processing carried out for profiling purposes. This is why it is extremely important for companies to demonstrate the steps they have taken to protect children and the safeguards they have put in place to prove their the lawfulness of their

44 See 'Creating a Better Internet for Kids | Shaping Europe's Digital Future' <<https://ec.europa.eu/digital-single-market/en/policies/better-internet-kids>> accessed 24 February 2020.

45 See Daniel Kardefelt-Winther, 'How Does the Time Children Spend Using Digital Technology Impact Their Mental Well-Being, Social Relationships and Physical Activity? An Evidence-Focused Literature Review. I How Does the Time Children Spend Using Digital Technology Impact Their Mental We' (2017) <www.unicef-irc.org> accessed 24 February 2020.

46 See for example 'Internet and Video Game Addictions: A Cognitive Behavioral Approach' <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0101-60832014000300082> accessed 24 February 2020.

47 See 'Study on the Impact of Marketing through Social Media, Online Games and Mobile Applications on Children's Behaviour | European Commission' (2016) <https://ec.europa.eu/info/publications/study-impact-marketing-through-social-media-online-games-and-mobile-applications-childrens-behaviour_en> accessed 24 February 2020.

48 See for example 'Gaming the System | Children's Commissioner for England' <<https://www.childrenscommissioner.gov.uk/publication/gaming-the-system/>> accessed 26 February 2020; 'Online Gaming | Childline' <<https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/online-gaming/>> accessed 26 February 2020.; 'The Games Industry Shouldn't Be Ripping off Children | Geraldine Bedell | Opinion | The Guardian' <<https://www.theguardian.com/commentisfree/2019/sep/15/games-industry-shouldnt-be-ripping-of-children>> accessed 26 February 2020. 'Online Games | NSPCC' <<https://www.nspcc.org.uk/keeping-children-safe/online-safety/online-games/>> accessed 26 February 2020.; see also *ibid.*; 'Media Moment: So Your Child Wants To Go To A Video Game Convention | Center on Media and Child Health' <<https://cmch.tv/media-moment-so-your-child-wants-to-go-to-a-video-game-convention/>> accessed 26 February 2020.; 'WHO Gaming Addiction Classification [Video]' <<https://finance.yahoo.com/news/world-health-organizations-new-classification-video-game-addiction-good-thing-220236312.html>> accessed 26 February 2020. "How the World Health Organization's new classification of video game addiction could be good thing"; Dr. Michael Rich discusses the behavior of teens and children with the popular game at "Fortnite" May Be a Virtual Game, but It's Having Real-Life, Dangerous Effects - The Boston Globe' <https://www.bostonglobe.com/metro/2019/03/31/unexplained-weight-loss-children-boston-nutritionist-makes-her-diagnosis-fortnite/eNMmGkK814IOsCwDDk2ZPN/story.html?s_campaign=8315> accessed 26 February 2020.; 'Kids and Smartphones and Video Game Addiction - Consumer Reports' <<https://www.consumerreports.org/gaming/kids-glued-to-smartphones-video-games-could-signal-addiction/>> accessed 26 February 2020.

practices.⁴⁹ The undeniable strong relationship between children's rights and online gaming industry is shown in UNICEF discussion paper, Child Rights and Online Gaming: Opportunities & Challenges for Children and the Industry⁵⁰. The open nature of the Internet and online gaming companies' inclusive approach to their consumers, without effectively separating children from adults can have serious impact on the children's exercise of their fundamental rights and freedoms. It is also noteworthy to note that depending on their age and maturity, children may find it difficult to identify the commercial nature of promotional content; therefore, it is important that all commercial content be clearly identified as such in a way that children can identify and comprehend without any struggle.⁵¹ In order to do this gaming companies need to have policies in place and take measures to make sure that advertising is effectively identified as commercial content.⁵² Overall, in the context of data protection and privacy, as children are a key consumer group for online gaming industry⁵³, to keep up with the laws and regulations, there is an absolute necessity to put additional safeguards in place in order to protect our children in the online gaming ecosystem.

II. Privacy Screening for Gamecell

This Section examines Gamecell's compliance with the core principles under the GDPR and KVKK for the purposes of accountability. To do so, it starts with Gamecell's User Agreement and continues with its Cookie and Privacy Policies to assess whether their content provided in these documents undermine children's rights to data protection and privacy under relevant laws. Although the main focus of this article is children's privacy, practices undermining adults' rights to data protection and privacy will be referred to where necessary. Also, references will be made to other laws and regulations (e.g.: law of obligations, e-commerce laws etc.) where necessary. Only the relevant terms and statements will be quoted in this article, which is then followed by and combined with our comments with regard to these provisions. This Section concludes that there is a big gap between theory and practice, and that Gamecell is far behind the expectations of the current data protection and privacy laws both under KVKK and the GDPR and there are missing steps which should urgently be taken in order to enhance children's rights and meet the expectations and requirements prescribed by law.

49 See ICO, 'The General Data Protection Regulation Children and the GDPR' (n 6).Pages 32-33

50 See Gorostiaga and others (n 42).

51 'CHILDREN'S ONLINE PRIVACY AND FREEDOM OF EXPRESSION' <[https://www.unicef.org/csr/files/UNICEF_Childrens_Online_Privacy_and_Freedom_of_Expression\(1\).pdf](https://www.unicef.org/csr/files/UNICEF_Childrens_Online_Privacy_and_Freedom_of_Expression(1).pdf)> accessed 18 February 2020. Page 24

52 *ibid.*

53 *ibid* page 5.

Gamecell's User Agreement

*Gamecell.Com "User" Agreement*⁵⁴

2. Establishment of the Agreement and Coming Into Effect

2.1: *"Agreement shall deemed to be established in a binding manner for the "User" beginning from the moment on which the "User" accesses to any content through creating or not any account information regardless of the duration of the transaction, visit, membership etc. and shall deemed to have been read, understood and approved by the "User"."*

According to Turkish Code of Obligations, a contract is established with bilateral and mutual declaration of the will of the parties. However, it is stated here that users' or visitors' mere access to the website is sufficient to form a binding contractual relationship. This proposition in the membership contract is against the Turkish Code of Obligations. If users want to become a member of Gamecell, they should be allowed to see, examine this contract separately and act accordingly in a way that they choose to do so by clicking to accept or not accept. In addition to this, this practice is a complete failure under the rules and principles set out in the GDPR, particularly 'consent'.

2.4: *"The "User" accepts that "Gamecell" solely has the right and authority to make partly or wholly changes, amendments, additions, updates on the terms of this Agreement in any time **without** giving prior notice, without having any seasonal or periodic, sectional or timing limitation arising from the reasons such as; the obligations occurred due to the technologies used on "Gamecell", new products and "Content"s to be presented, liabilities arising from the changes in the legislation, updates, partly or wholly changes to be made on the current products, services and "Content"s; and the "User" shall not claim, demand or declare not being notified or that the aforesaid changes are not applicable for him/herself in case "Gamecell" informs the "User" directly or in case the "User" accesses to "Gamecell" at a date later than the occurrence of the amendments or updates. Furthermore, in order to use any service, content, technology on "Gamecell", the "User" may be required to accept certain software or content or other usage terms; the "User" accepts to benefit from the services and contents by knowing such situation."*

Since the contract expresses mutual declarations of intention to create legal relations and a mutual will, these changes must be brought to the attention of the user and the acceptance/rejection options must be provided accordingly. This practice can be considered to be unfair and regarded as an abuse of imbalance of powers as explained above in Section I.

54 'Gamecell - Oyunlar. Arkadaşlar. Eğlence.' <<https://www.gamecell.com/tr/userAgreement.html>> accessed 26 February 2020.

3. Liabilities and Responsibilities of the User

3.6: *"The "User" accepts, declares and undertakes to deal with the advertisements belonging to third persons or institutions having a content of commercial communication during, before or after the use, benefit or trying to access to the "Content" and services presented by "Inteltek" on "Gamecell" or "Content"s services accessed through "Gamecell" and/or any sort of other services directly or indirectly in relation with them; and that the access to "Content" may be prevented, slowed down or stopped without watching/viewing these advertisements, and that "Inteltek" has the sole right and authority to make partial or total changes, amendments, additions and updates in this process."*

This can be done; however, the explicit consent of the user is required for targeted advertising. Also, as it can be seen in ICO's report, legitimate interest is dismissed as a legal basis for processing personal data for the purposes of advertising based on user profiles.⁵⁵ It is also noteworthy to recall that profiling requires obtaining consent from data subjects, and the obtained consent must be informed, explicit and freely given for the purposes of the GDPR. With regards to children, if processing activities are likely to result in a high risk to the rights and freedoms of children, then a DPIA is required.⁵⁶ As it can be seen in the ICO's guidance, the use of children's personal data for marketing purposes, profiling or other automated decision-making, or if data processing carried out if there is an intention to offer online services directly to children, then it means that a DPIA is required to achieve the purposes of data protection regime.⁵⁷

5. Ownership of Other Accessible Contents

5.1. *"By visiting "Gamecell", the "User" accepts that it is possible to access from "Gamecell" to any sort of digital media, website, product or contents including with the advertisements belonging to third persons."*

There is no such requirement for hosting service providers set out under the Law No 5651. Obligations of the hosting service provider ARTICLE 5- (1) The hosting provider shall not be responsible for checking the content which it is hosting, or investigating whether or not it constitutes an unlawful activity. (2) (Amended: 6/2/2014-6518/article 88) The hosting provider must remove hosted content which is unlawful when notified in accordance with articles 8 and 9 of this Law. (3) (Annex: 6/2 / 2014-6518/Article 88). The hosting providers are required to retain traffic data (communications data) in relation to their hosting activities from one to two years (Article 5(3)) and access providers for a period of not less than six months and not more than two years and ensure the accuracy, integrity and confidentiality of this information.

55 See 'Examples of Processing "Likely to Result in High Risk" | ICO' <<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/examples-of-processing-likely-to-result-in-high-risk/>> accessed 26 February 2020.

56 See 'What Should Our General Approach to Processing Children's Personal Data Be? | ICO' <<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr/what-should-our-general-approach-to-processing-children-s-personal-data-be/>> accessed 26 February 2020.

57 See 'Examples of Processing "Likely to Result in High Risk" | ICO' (n 55).

10.6. “*“Inteltek” shall not be held liable against the “User” from the consequences of being forbidden to use “Gamecell” “Content” and services pursuant to the legislation in force in the country or region where the “User” is located, regardless of the beginning date to benefit from this service and “Content” s.*”

This provision is unacceptable under the EU data protection law. Gamecell’s website is designed in a way that is accessible in both English and Turkish. This means that users (adults and children) residing in Europe as well as other parts of the world can access the website and sign up to become a member. Pursuant to Article 3 (Territorial scope) of the GDPR, the Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.⁵⁸ Therefore, it can be concluded that Gamecell is subject to the principles and rules set out under the GDPR since its products and services are accessible in Europe.

11. Cookie Policy, Privacy Policy and Protection of Personal Data

Cookie Policy

11.1 “*...Within this scope, the right of sending cookies of the advertisers and the payment system providers of “Gamecell” is reserved and even they are registered or not, the “User” s are deemed to be agreed on the cookie policy/application of “Gamecell” determined in this Agreement.*”

The Cookie Policy cannot be forced on to be accepted as default in this way. This Policy should provide information about cookies; when the user accesses the Gamecell home page, he/she should be informed about the cookies with the consent management tools and his explicit consent should be obtained. An option to change the preferences about cookies should always be provided on the website and data subjects’ rights and their freedom of choice should not be undermined. Again, this provision can be considered as an abuse of the imbalance of power and therefore can be deemed unfair. It is also relevant to note that such an approach will not only be considered as a failure to comply with the relevant rules and principles under data protection and privacy laws, but also will contradict with the purposes of Unfair Contract Terms Directive.⁵⁹ This is because although the rest of the agreement remains valid, conditions that are deemed unfair are not binding on consumers under the Unfair Contract Terms Directive.⁶⁰

58 See EDPB (n 19); note that Article 3 of the GDPR provides as follows: “*Article 3 – Territorial scope (1) This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not. (2) This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or the monitoring of their behaviour as far as their behaviour takes place within the Union. (3) This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.*”

59 ‘European E-Justice Portal - Unfair Contract Terms Directive (93/13)’ (n 37).

60 See *ibid.*

11.1 *"...The right to update the applications regarding cookies by publishing via "Gamecell" is reserved and it's under the "User"'s liability to follow and have knowledge about aforesaid updates."*

No such obligation can be imposed on the user. Changes to the cookies and the policy should be made available to the user, along with the version and update date.

11.2. *"The "User"s may deactivate/passivate "cookie" sections of their web browser in case the "User"s do not want to deal with the cookie applications explained below. (For example, the "User" may reject all of the cookies by clicking "Tools", "Internet Options", "Privacy" sections and marking "Block all cookies".)"*

It is necessary to manage this with the privacy management tool to be provided on the homepage of the website and act according to the will of the user. It is not sufficient to include such a provision in the contract. This provision should be put into practice and implemented duly for the purposes of Accountability.

11.3 *"Google, as "Gamecell" advertiser, uses cookies to publish advertisements on "Gamecell" and may present advertisements based on the visits of the "User" to "Gamecell" and to other websites on internet by using "DART" cookies."*

The platforms that children use should be ad-free. Here, the YouTube decision can set an example for Gamecell to learn lessons from the FTC's statements⁶¹ about ad-free platforms for children as it will be explained more in detail in Section III.

11.4 *"The usage of "Google Analytics" and any similar technology is also possible in order to make the analysis of the visitors "Gamecell" usage. "Google Analytics" enables to acquire statistical and other type of information about the usage of a website via cookies stored in the computers of the visitors and is used to create relevant reports regarding the use of "Gamecell". To receive further information about "Google Analytics" technology, you can visit <https://www.google.com/intl/tr/policies/privacy/> The "User" declares and undertakes in advance that any other type of similar technology and/or technological infrastructure which is owned by third parties apart from "Google Analytics" may be used in the future."*

Making the user declare and undertake in advance that any other type of similar technology which is owned by third parties to be used in the future is unacceptable and is out of the question. The content of this term is unacceptable for many reasons since it contradicts with the essence of the data protection and privacy regimes in general. It is known that analytics cookies are subject to explicit consent, a user cannot be assumed to have accepted by default their usage as it is the case now.

61 See 'Google and YouTube Will Pay Record \$170 Million for Alleged Violations of Children's Privacy Law | Federal Trade Commission' <<https://www.ftc.gov/news-events/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations>> accessed 26 February 2020.

11.5 “...by accessing “Gamecell” as subscriber or nonsubscriber can be saved via “cookie” technology in order to be used at the advertisement applications or presentations without any requirement to obtain any of the “User”’s personal data...”

All cookies collect personal data. For this reason, the owners of cookies and similar technologies and those using these technologies are deemed to be responsible for data collected and are required to comply with the rules set out under the KVKK and the GDPR.

11.5 “In addition, Internet Protocol (IP) numbers assigned by internet service providers of the “User”’s may be used for advertising display purposes or for security reasons (for example, to identify any attacks on “Gamecell”, or to be shared with governmental authorities in case of a criminal complaint or a request for official investigation against the “User”).”

Targeted advertising is a crucial topic for the purposes of data protection law. One of the main reasons lies at the heart of the term ‘invisible tracking’ as it confronts us with vague, ambiguous, non-transparent, and opaque personal data processing activities that is called invisible tracking. It is noteworthy to mention that in the context of advertising; protection of children has become more under the spotlight recently. In the targeted advertising ecosystem, the current practices for implementation of the consent requirements under the GDPR should be applied carefully as failure to meet the requirements can have serious effects on children with regards to data protection and privacy laws. Accordingly, the legal and ethical implications of the advertising ecosystem’s practices call for additional care and careful consideration of the potential effects they can create on children.

11.6 “...while the persistent cookies are used to enable “Gamecell” to remember the “User” and to determine the last games that the “User” had played..”

Since Gamecell is a platform that users can benefit from, when they make a payment for such services, it can be considered as offering service for the information society and therefore can use cookies for secure login and logout. Strictly necessary cookies are essential for you to browse the website and use its features, such as accessing secure areas of the site.⁶² Strictly necessary cookies which are used for the functionality of the website can be placed before the user’s affirmative action.⁶³ The exact scope of “strictly necessary cookies” is not clearly defined; however, it can be said that such cookies are the ones that are essential for the user to receive the service he/she requests.⁶⁴ In November 2009, the European Union introduced various amendments to the existing Directive 2002/58/EC (e-Privacy Directive), including to the provisions regulating the use of cookies. Following these changes, the e-Privacy Directive required obtaining

62 ‘Cookies, the GDPR, and the EPrivacy Directive - GDPR.Eu’ <<https://gdpr.eu/cookies/>> accessed 26 February 2020.

63 See ‘Consent on the Internet Means “Opting-in” in Europe’ (2019) <www.hoganlovells.com> accessed 26 February 2020.

64 See ICO Guidance ‘Privacy and Electronic Communications Regulations Guidance on the Rules on Use of Cookies and Similar Technologies Contents’. “The term ‘strictly necessary’ means that such storage of or access to information should be essential, rather than reasonably necessary, for this exemption to apply. However, it will also be restricted to what is essential to provide the service requested by the user, rather than what might be essential for any other uses the service provider might wish to make of that data.”

the consent of users in order to store or access information (typically cookies or similar tracking technologies) on their devices. The only exemptions to this requirement are where this is for the sole purpose of transmitting a communication or where it is strictly necessary to provide an internet service explicitly requested by the user.⁶⁵ It is also important to note that if a company categorized a cookie they collect as "strictly necessary" because it fulfils a specified objective like security, it should make sure that cookie is solely used for that specific purpose. This approach is also aligned with the approach of the principle of purpose limitation under Article 5(1) of the GDPR. If any information is used for secondary purposes, the cookie would not be regarded as strictly necessary and therefore such use would require consent.⁶⁶

12. Consent

12.1. *"Unless the "User" uses its right of refusal, The "User" accepts and declares giving an indefinite approval (even this Agreement is terminated) in favor of "Inteltek" and/or in favor of the institutions which are in cooperation with "Inteltek" to send commercial electronic messages (having data, voice and image content and which are sent through telephone, call centers, facsimile, automatic calling machines, smart voice recorder systems, email, small message services for commercial purposes) pursuant to the Law on the Regulation of Electronic Commerce numbered 6563 ("Law") and the Regulation on Commercial Communication and Commercial Electronic Messages for the purposes of declaring general/special possibilities and promoting and marketing various and new products-services in relation to the services and "Content"s provided under "Gamecell" through the contact information provided by the "User" while registering to "Gamecell"."*

This is completely against the e-commerce legislation. The above explained reasons are applicable in this case as well.

12.2. *"By using "Gamecell" "Content" and services, the "User"s are deemed to be agreed that the email and SMS notices or advertisements subject to this article are sent within their own consent and will and do not constitute violation or illegal saving of personal data, offensive advertisement, unfair competition or marketing."*

It cannot be claimed that all of the obligations arising from e-commerce and KVKK legislations are fulfilled and the user accepts this merely because the services provided by Gamecell are used. All these processes should be designed in accordance with the relevant legislation.

15.2. *"Any kind of "User" transaction made on "Gamecell" and their transaction costs, if exists, are at the disposal and responsibility of the "User"."*

⁶⁵ *ibid.*

⁶⁶ See 'What Are the Rules on Cookies and Similar Technologies? | ICO' <<https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/what-are-the-rules-on-cookies-and-similar-technologies/>> accessed 26 February 2020.

Taking into account the fact the users can be children, processes and provisions should be designed in accordance with the legislation in terms of transactions that will lead to legal consequences.

16. Content Compatibility

16.1. *“The ‘User’ is entitled to control and decide on the appropriateness of all kinds of games, publications, ‘Content’ and other elements, especially the appropriateness of the games on ‘Gamecell’ or accessed through ‘Gamecell’ to the age groups. ‘Inteltek’ may share with the ‘User’ the evaluations, if exists, made by the competent public authorities regarding the appropriateness of the ‘Contents’ on ‘Gamecell’ to the age groups provided that being non-binding.”*

Not providing appropriate content for specific age groups as it is the case in Pan European Game Information (“PEGI”) and let the children decide what game to play is unacceptable as it is not fair nor lawful for the purposes of data protection regime. Here, the below explained PEGI standards should be referred to keeping in mind the tangible effects of games that are inappropriate for certain age groups.

16.2. *“If the age of the ‘User’ is below the legal age limit; it is strongly recommended to the ‘User’ to notify the ‘Content’ to its legal representatives before exploiting from these ‘Contents’, to ask the appropriateness of the chosen ‘Contents’ for the ‘User’'s age group and to exploit, use and continue to use the ‘Content’ in connection with the ‘User’'s legal representatives approval.”*

The platform is and should be responsible to take the necessary steps in order to provide lawful, transparent and fair processing of data especially when the children are concerned. Also, for the purposes of the data protection regime and the novel principle of accountability under the GDPR, it is a no brainer that Gamecell should demonstrate that the necessary steps are taken in order to provide adequate protection to the most vulnerable group of the society, children. In this regard, Gamecell should make a genuine effort to take solid steps, make tangible changes in its practices to ensure (to the best possible extent) identify that the user is a child and that parental consent is obtained for child's use of its services.

16.3 *“It is recommended for the ‘User’'s who do not fulfill this requirement to be accompanied by permission and supervision of their legal representatives related to the relevant transactions and acquisitions and the related transactions are deemed to be carried out in this way.”*

Gamecell should clarify how and with which methods this is going to be controlled.

Gamecell's Cookie Policy and Privacy Policy

Cookie Policy, Privacy Policy and Protection of Personal Data⁶⁷

COOKIE POLICY 1.1: "... the "User"'s visits on the internet can be observed before, during or after their access to the "Content"'s on "Gamecell" and advertising applications can be realized to the "User" accordingly."

Considering that most of the users are children, this leads us to the same conclusion with the YouTube decision.⁶⁸ Children should not be subject to profiling with cookies and similar technologies and online platforms that are accessible to and used by children such as YouTube Kids should therefore be free from ad-free and tracking tools.

1.1 "...the right of sending cookies of the advertisers and the payment system providers of "Gamecell" is reserved and even they are registered or not, the "User"'s are deemed to be agreed on the cookie policy/application of "Gamecell" determined in this Agreement."

In terms of consent, the website works as opt-out. It automatically considers as if children have accepted default cookies and third party cookies without obtaining their prior consent. This practice is unacceptable under the applicable data protection and privacy regimes.

1.1 "The right to update the applications regarding cookies by publishing via "Gamecell" is reserved and it's under the "User"'s liability to follow and have knowledge about aforesaid updates."

It is not fair nor lawful to impose a duty to act on any user including children as well as adults. Obtaining a valid consent and making sure that its practice is in compliance with the relevant rules and principles is the responsibility of the game platform.

1.2: "The "User"'s may deactivate/passivate "cookie" sections of their web browser in case the "User"'s do not want to deal with the cookie applications explained below. (For example, the "User" may reject all of the cookies by clicking "Tools", "Internet Options", "Privacy" sections and marking "Block all cookies".)"

This practice is also unacceptable as the information about how to opt-out is provided after the user starts using the website. In good practice, consent should be obtained prior to such use. This is because the cookies are already being used before the user (in our case, the child) is informed about rejecting cookies option.

1.3: "Google, as "Gamecell" advertiser, uses cookies to publish advertisements on "Gamecell" and may present advertisements based on the visits of

67 'Gamecell - Oyunlar, Arkadaşlar, Eğlence.' <<https://www.gamecell.com/tr/privacyPolicy.html>> accessed 26 February 2020.

68 'Google Is Fined \$170 Million for Violating Children's Privacy on YouTube - The New York Times' <<https://www.nytimes.com/2019/09/04/technology/google-youtube-fine-ftc.html>> accessed 26 February 2020.

the “User” to “Gamecell” and to other websites on internet by using “DART” cookies. By visiting “Google Privacy Policy” on <https://www.google.com/intl/tr/policies/privacy/>, the “User”s may block the use of DART cookie.”

1.4: *“The usage of “Google Analytics” and any similar technology is also possible in order to make the analysis of the visitors “Gamecell” usage. “Google Analytics” enables to acquire statistical and other type of information about the usage of a website via cookies stored in the computers of the visitors and is used to create relevant reports regarding the use of “Gamecell”. To receive further information about “Google Analytics” technology, you can visit <https://www.google.com/intl/tr/policies/privacy/>.”*

Similar concerns arise in 1.3 and 1.4 from the practices explained above.

1.4: *“.....The “User” declares and undertakes in advance that any other type of similar technology and/or technological infrastructure which is owned by third parties apart from “Google Analytics” may be used in the future.”*

This practice conflicts with the rules relating to consent under KVKK and the GDPR. It is not clear which product will be used in the future; to obtain approval, or so-called “consent” from the users for an uncertain future situation fails to be as a valid consent for many reasons including the lack of elements such as being explicit and specific. Consent means offering individuals real choice and control. Thus, the case at hand contradicts with such an approach as genuine consent should put users in charge, build trust and real engagement.⁶⁹ It is noteworthy to state that there is a need to be specific and ‘granular’ so that separate consent is obtained for separate purposes of processing. In this context, consent taken for unknown (not specific enough) potential use in the future use can be regarded as vague failing to be specific. As provided under the current data protection law regime, vague or blanket consent is not enough.⁷⁰ Also, such a practice cannot be considered as fair, lawful nor transparent for the purposes of Article 5(1)(a) under the GDPR. Here, the principles of purpose limitation and data minimization also become highly relevant. This is also important for compliance with the consent rules under the GDPR, which requires consent to be specific and informed in order to be considered valid. Furthermore, it means that the potential consequences of giving consent should be made clear. To elaborate, the user must be presented with any information that is necessary to understand what he/she is consenting to without being pushed into agreeing with a term that fails to specify the details about what is referred to as “any other type” or is made even more ambiguous by the use of “in the future”.

1.5: *“.....can be saved via “cookie” technology in order to be used at the advertisement applications or presentations without any requirement to obtain any of the “User”’s personal data.”*

⁶⁹ ‘Consent | ICO’ <<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/>> accessed 26 February 2020.

⁷⁰ *ibid.*

This statement is misleading and fails to be true since the data collected through the use of cookies constitute personal data.

1.5 *".....The purpose of this technology is to make it easier for the "User" to access to the content of the sections that the "User"s are visiting more frequently from their first visit to "Gamecell" and to provide suitable advertisements for the "User"s."*

If the real purpose of data collection is delivering ads, the data protection and privacy regimes made it clear enough by setting out what steps should be taken in order to comply with the rules and principles laid out under the law.

1.5 *".....In addition, Internet Protocol (IP) numbers assigned by internet service providers of the "User"s may be used for advertising display purposes or for security reasons (for example, to identify any attacks on "Gamecell", or to be shared with governmental authorities in case of a criminal complaint or a request for official investigation against the "User")."*

It has been recognised that IP addresses constitute personal data.⁷¹ According to Law No. 5651, only traffic data can be processed with the obligation to store it for 2 years. However, it cannot be used to show ads.

1.6. *"In case the web browser is closed, then session cookies are deleted, while persistent cookies are stored until the reasons for data processing are removed."*

The details about such data processing including storage durations should be shown in a table.

Security, Privacy Policy and Protection of Personal Data⁷²

1.7 *"In case that the "User" wishes to use "Gamecell" by registration, the "User" accepts to give true and complete information while opening an account, doing registration in any way and using "Contents" and services on "Gamecell" and to update these registry informations in order to keep them true and complete. In case that the "User" wishes to use "Gamecell" by registration, the "User" shall be subject to the regulations determined for membership under this Agreement; while being subject to the below stated terms and conditions for his/her personal datas."*

There is a need to specify which personal data is asked for what specific reason. The current practice is not compliant with the GDPR for many reasons including the principles of purpose limitation and 5(1)(a). Accordingly, this also leads to a failure to comply with the accountability principle set out under Article 5 (2).

71 See 'What is personal data?' (European Commission) <https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en> accessed 29 January 2020. Also note that The European Court of Justice ("ECJ"), Breyer, in its October 2016 verdict, decided that "personal data" *"must be interpreted as meaning that a dynamic IP address registered by an online media services provider when a person accesses a website that the provider makes accessible to the public constitutes personal data within the meaning of that provision, in relation to that provider; where the latter has the legal means which enable it to identify the data subject with additional data which the internet service provider has about that person."* See Case C-582/14, Patrick Breyer v. Bundesrepublik Deutschland [2016] ECLI:EU:C:2016:779.

72 'Gamecell - Oyunlar. Arkadaşlar. Eğlence.' (n 67).

1.10 *“Inteltek” only provides the information delivered by the “User”s ownself and their own will. The “User”s may visit “Gamecell” at any frequency without being registered and sharing personal information.”*

Details should be given with regards to the information collected from the users. In other words, the company should clarify what data is being collected. Allowing an option to visit Gamecell as a guest, without creating an account is good practice for the purposes of the rules under the GDPR and respect for data subjects’ rights.

1.11 *“Pursuant to the “Law on the Protection of Personal Data”, “Gamecell” may process the informations conveyed by the “User” basing on the “User”s’ approval or express consent conveyed during registration by stating “in case that I become a member of this Website via approving this user agreement, I accept giving authorization to the procession of my data” and “Gamecell” may classify and protect these informations. These informations are used for marketing of the products and services of “Gamecell” and/or companies determined by “Gamecell” and used for the purpose of statistical examination, database enlargement, campaign organization, management of “Gamecell”, improvement of the “User”s’ browsing experience while personalizing “Gamecell”, enabling the “User” to use the services which are utilizable on “Gamecell”, procurement of statistical informations related with the “User” to third parties in a manner not to be used to identify any “User”, dealing with the complaints made by the “User” related to “Gamecell” or dealing with the complaints made against the “User” to “Gamecell” and etc.”*

There is no need to obtain explicit consent with regards to the processing carried out in the context of a contractual relationship and comply with the Articles 5(f) and 2(c) under KVKK.⁷³ In this context, provision of a privacy notification is sufficient. In addition, it is unlawful to ask for users’ consent for the processing carried out in the context of a lawful basis that is recognised under the law. This is because, in a way, such an act would amount to misleading, misdirecting one’s free will. Also, it is noteworthy to state that the listed points here, namely, organizing campaigns; marketing of Gamecell products and services; marketing of the products and services of companies to be determined by Gamecell all require explicit consent in accordance with e-Commerce legislation. This is also relevant under Articles 5 and 7/f.5 according to the updated commercial electronic messaging regulation. Also, the wording that is used in the above paragraph, more explicitly the phrase of “in a manner not to be used to identify any User” means that Gamcell anonymizes the data it collects from users. However, as it has been widely recognised in the studies, what usually may seem as anonymous is pseudonymisation. The ICO also confirms and underscores that the entities ‘frequently refer to personal data sets as having been “anonymized” when, in fact, this is not the case’.⁷⁴ In light of this, it becomes even more crucial for companies to explain how they carry out their anonymization. In other words, the tools used to transform personal data

73 See ‘AÇIK RIZA’ <<https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/66b2e9c4-223a-4230-b745-568f096fd7de.pdf>> accessed 26 February 2020. for further detail about explicit consent under the KVKK.

74 ICO, What Is Personal Data? (2019), <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-is-personal-data>. (Accessed 30 January 2020)

into anonymous data should be clarified for transparency purposes.

1.12: *““Gamecell” is authorized to let “Content” providers and web services users to use personal informations conveyed by the “User” for the purposes of required contact, display, product delivery, advertisement etc. providing that they are not used in a manner which do not violate the “User”s personal rights. In other words, the “User”s accept that the collected datas and informations within the scope of this Agreement may be shared and/or transferred to the employees, service providers, group companies and/or existing and/or potential business partners of “Gamecell” and both of these situations shall not be deemed as a violation within the scope of this article. By registering to “Gamecell”, the “User” shall deemed to be agreed and showed his/her express consent pursuant to the “Law on the Protection of Personal Data” basing on the approval in this respect conveyed as “in case that I become a member of this website via approving this user agreement, I accept giving authorization to the procession of my data” while registering to the “Website”. Without prejudice to the provisions of this Agreement, “Gamecell” shall not share certainly with third persons the personal informations obtained within the scope of this Agreement, in a manner violating the “Law on the Protection of Personal Data” or apart from the conditions of this Agreement and shall not use for commercial purposes in any non-operating reason.”*

According to what is stated in the above paragraph: who are the content providers and web service users?; what are the personal rights of the member/user? Also, obtaining explicit consent from the user is required in order to be able to share data for the purpose of communication, promotion, delivery of goods and advertisements for content providers and web service users. This matter does not comply with the other rules that are deemed lawful under Article 5 of the KVKK. Pursuant to the applicable law, it is not possible to state that the consent covers both domestic or international data transfers, based on the explicit consent that the user gave when signing up to Gamecell; it is also noteworthy to state that the consent in question is not actually obtained in compliance with the law and therefore should not be considered as a valid consent for the purposes of the data protection regime. In particular, it is not possible to accept the following sentence of the paragraph: *“In other words, the “User”s accept that the collected datas and informations within the scope of this Agreement may be shared and/or transferred to the employees, service providers, group companies and/or existing and/or potential business partners of “Gamecell” and both of these situations shall not be deemed as a violation within the scope of this article.”* This sentence is contrary to the core elements constituting an explicit consent, being specific, unambiguous, and legitimate. In this case, it is assumed that the user gives consent by default to data processing purposes other (transfer of data) than the main purpose (subscription) for which user’s consent is taken, which already fails to meet the requirements set out under the law, and therefore is unlawful. It is a no brainer when the user signs up for the services provided, there is a need to obtain an explicit consent separately for transfer of data which should be regarded as different than the consent given for subscription purposes. In other words, apart from the consent obtained for membership to the site, it will be necessary to obtain

consent for cases where an explicit consent is required for data transfer. However, it is unlawful and unfair to assume that the consent given for membership purposes without this is actually accepted as a consent given for data transfers and that the user will be deemed to have accepted this matter by clicking on the membership agreement. In addition, stating that the company's practice should not be considered as a violation under this Agreement is contrary to the basic principle of "*Lawfulness and conformity with rules of bona fides*"⁷⁵ under Article 4(2)(a) of the KVKK.

1.13 *"In order to provide top level security for the "User"s who make shopping on "Gamecell" during their transactions requiring Virtual Pos/Credit Card payment option,....."*

The majority of Gamecell users are children. Taking this into consideration, it is necessary to obtain parental consent for those under the age of 18 for payment. Otherwise, it would mean that a child under the age of 18 will make a legal transaction, an act recognised in law, without the consent of his/her parent(s). This means that, in the future, the cancellation of the transaction may be necessary when the child's parent(s) declares that he/she has not approved this payment.

1.15 *"...data regarding location details may be used with a separate approval of the "User"."*

This is compliant with Article of 51(6) of the Electronic Communication Law⁷⁶, without prejudice to the relevant legislative provisions regarding the transfer of personal data abroad, traffic and location data can only be transferred abroad when explicit consent of data subject is obtained.

1.16 *"In case the message is unencrypted during email communications, the "User" is responsible from the security of the emails to be sent, as the security of the message cannot be guaranteed."*

There are questions that need to be addressed in this context such as: How will the necessities be fulfilled for users (including children and adults)? Why is there a need for encryption? Which encryption algorithm should be used to encrypt mails? The answers to these questions are not made clear for users, which is against the transparency principle.

1.17 *"The "User"s accept and undertake that the "User" has got the required permissions from the owners of the personal right related to the personal informations in the "Content"s and informations related to private life of persons and/or in terms of "Content"s and that the "User" shall not use within the scope of "Gamecell" the "Content"s and informations protected by any sort of intellectual and industrial property right including other ownership rights which violates any others personal right, right of privacy or right of publication without taking prior*

75 'Processing of Personal Data General Principles'.

76 See 'ELEKTRONİK HABERLEŞME KANUNU 5809' (2008) <<https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5809.pdf>> accessed 26 February 2020.

written consent from the owner or holder of these rights. Otherwise, the "User" accepts and undertakes to be held liable from any criminal and legal responsibility which will arise."

What are the situations in which a user using the Gamecell platform should share personal data belonging to someone else and information about and content about someone else's private life? In the first place, these should be explained clearly and then the rule of acting in accordance with this law should be reminded.

1.18 *"The "User" who becomes a member of "Gamecell" by approving this "Agreement", clearly approves the commercial electronic messages to be sent to himself/herself and to the saving, process, transfer and sharing under the "Law on the Protection of Personal Data" of the personal data transmitted for the registration to "Gamecell"."*

This term contradicts with both e-commerce and data protection legislations. Pursuant to Article 7(f)(5) (Obtaining Approval) of the Regulation on Commercial Communication and Commercial Electronic Messages, if an approval that is included in a contract such as subscription, sales and membership contract, at the end of the contract, before the positive declaration or before the signing takes place, such an approval should be taken under the commercial electronic message title by giving the other party the option to reject, written in at least twelve font size. Accordingly, it can be concluded that this term included in the Gamecell membership agreement is in violation of Article 7(f)(5). In addition, while the personal data processing carried out for the purpose of establishing or executing a contract does not require explicit consent pursuant to Article 5(f)(2) of the KVKK, under Article 5 of the Regulation on Commercial Communication and Commercial Electronic Messages sending a commercial electronic message requires approval.⁷⁷ For this reason, it is not lawful to create a presumption the user with a provision to be included in the membership contract, deeming the user to have accepted a matter that requires an explicit consent. The Gamecell membership contract is also a distant contract and is set up by clicking. For this reason, the matters requiring sending of commercial electronic messages and other explicit consent, should be placed under the membership contract in separate boxes, and these boxes should be empty and not presented to the will of the user as pre-checked.

1.20: *"The "User" may transmit any of his/her requests regarding the application of the "Law on the Protection of Personal Data" and any of his questions regarding his/her personal datas in written form (notarized, registered letter with return receipt) to Uniq İstanbul, Huzur Mah. Maslak Ayazağa Cad. No: 4/B – 601 Kat: 5 34396 Sarıyer/İstanbul which is the headquarters address of "İnteltek"."*

According to Article 5(f)(1) of the Communiqué on the Procedures and Principles of Application to the Data Controller which regulates the application procedure for the data controller; "The data subject concerned uses his/her requests within the scope

⁷⁷ 'TİCARİ İLETİŞİM VE TİCARİ ELEKTRONİK İLETİLER HAKKINDA YÖNETMELİK' (Resmî Gazete Sayısı: 29417, 2015) <<https://www.mevzuat.gov.tr/Metin.Aspx?MevzuatKod=7.5.20914&MevzuatIliki=0>> accessed 26 February 2020.

of his rights specified in Article 11 of the Law, in writing or by registered electronic mail (KEP) address, secure electronic signature, mobile signature or the e-mail address previously reported to the data officer by the person concerned and registered in the system of the data officer. It transmits to the data controller by means of a software or application developed for the purpose of application". Accordingly, since the e-mail addresses of users who are members of Gamecell are already registered in Gamecell, the applications that are sent in scope of Article 13 of the KVKK using this email address will need to be accepted and replied by Gamecell. It is also a requirement of the principle that the data controller should be "accountable" not to direct the user to more severe, difficult and time-consuming methods in order to use the rights on his personal data, especially in distant contracts that are established very easily and quickly by clicking.

16.4. *"Any legal relation or commitment between the "User" and other real person or institution, arising from the "Content" and services presented on the "Gamecell", is not guaranteed and the interpretation of this Agreement in this manner is rejected by "Inteltek". "Inteltek" makes every effort to provide systematic security of any kind of information that the "User" holds in relation to "Gamecell". However, this can not be interpreted under any circumstances as the unlimited liability of "Inteltek" from the "User" accounts, the security of the account access information and other "Gamecell" "Content"."*

Under Article 12 (Obligations concerning data security) of the KVKK, it is provided that the controllers are obliged to take all necessary technical and administrative measures to provide a sufficient level of security in order to: a) prevent unlawful processing of personal data, b) prevent unlawful access to personal data, c) ensure the retention of personal data.

21.1 *"The "User" shall not assign any of his rights and authorities that he directly or indirectly holds on the services or "Contents" provided on "Gamecell" or within the scope of this Agreement to any third parties without taking written consent of "Inteltek"."*

Children should be taken into account and this term should be changed and in fact rewritten.

22. Applicable Law

22.1. *"Any disputes arising out of the implementation of this Agreement shall be resolved by Istanbul Caglayan Courts and Execution Offices and the books and records of "Inteltek" shall be deemed as exclusive evidence. The laws of Turkish Republic shall be applied for the settlement of disputes arising out of the application of this Agreement, except for the conflict of laws rules."*

As explained above, pursuant to Article 3 (Territorial scope) of the GDPR, the Regulation applies to the processing of personal data in the context of the activities of

an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not. Therefore, it can be concluded that Gamecell is subject to the principles and rules set out under the GDPR since its products and services are accessible in Europe.

22.2 *"In case 'Inteltek' has not been able to provide a solution or the offered solution does not found suitable for 'Gamecell' then the 'User' will reserve its right to appeal to the consumer court or to the consumer arbitration committee located at his residential area or at the place where the purchase is realized by considering the product amount."*

The above comments are also relevant here.

Concluding Remarks

Overall, in light of the above analysis, although privacy policies, cookie policies are usually found to be confusing, in this case, Gamecell's user agreement and policies are not even close to be inconspicuous and difficult to understand. In fact, the choice of words, phrasing and the overall content of certain provisions are shamelessly clear enough enabling one to see straight away that there are unacceptable mistakes and intolerable practices in the context of data protection and privacy regimes. As a result, following our analysis and review of Gamecell's User Agreement and its Cookie and Privacy Policies, we conclude that Gamecell should urgently take steps to ensure that the necessary changes are reflected into their policies and are implemented according to the rules and regulations in their practice. Below we will explain the recent developments and trends in the world which can be helpful not only to Gamecell, but to all online platforms in practice for the purposes of protecting children's rights and ensuring that they take the necessary steps and therefore can demonstrate their compliance with the data protection and privacy laws. A mistake that can be observed in its practices is the misunderstanding or lack of knowledge of Article 3 of the GDPR. Most of the above chosen terms and statements undermine data protection law's aim to protect fairness and fundamental rights when personal data are processed. Again, in many of the above mentioned statement, the goal of protecting people against abuse of information asymmetry⁷⁸ seems to be overlooked.⁷⁹ It is also important to note that privacy policies and terms of service are generally drafted from the service provider's perspective. An ideal practice would be taking into account the users' perspectives and be more inclusive in the sense that providing explanations for both children and adults, but also more discriminatory in the

78 See De Hert and Gutwirth, "Privacy, data protection and law enforcement: Opacity of the individual and transparency of power" in Claes, Duff and Gutwirth (Eds.), *Privacy and the Criminal Law* (Intersentia, 2006); Zuiderveen Borgesius, *Improving Privacy Protection in the area of Behavioural Targeting* (Kluwer Law International, 2015), Ch. 4, section 4, and Ch. 7. Cited in https://www.ivir.nl/publicaties/download/CMLR_2017.pdf

79 See also <https://www.isfe.eu/wp-content/uploads/2018/11/ISFE-Response-ICO-Guidance-on-Children-and-the-GDPR-2018.pdf>

sense that the language used can be different for children. Also, policies and terms of services are often focused on addressing the legal risks and obligations of the provider, written “*in legalistic language and forcing users to accept terms to access the service*”.⁸⁰ Such a practice ultimately leaves children with little choice but to provide the information and give consent as asked; therefore, this approach calls for careful consideration and creates concerns as to it amounts to ‘forced consent’ and thus fails to be valid consent.⁸¹ Additional care is required under the GDPR for the form in which the information should be given to children, namely in “*such a clear and plain language that the child can easily understand*.”⁸² It is also important to take the Interactive Software Federation of Europe’s (ISFE) concerns into consideration, highlighting that the ICO’s Guidelines recommendation of online gaming companies’ provision of different versions of the privacy notice when “*the target audience covers a wide age range, even in cases where parental consent is triggered as the lawful basis*” can be problematic in practice and such a recommendation creates confusion on their parts under Article 8 of the GDPR.⁸³ Therefore, instead of trying to comply with the relevant laws and regulations by adopting a literal interpretation approach of the available provisions, the essence lying at the heart of the data protection regime should be understood. This is where the notion of fairness becomes highly relevant to comprehend. Therefore, in whatever decision the online gaming company takes, the question of whether the decision will involve or has the possibility to involve children should be asked and then the activity or the decision should be considered from looking at the lenses of the notion of ‘fairness’. Furthermore, such an approach would enhance the position of children in a society and allow them to exercise their rights and freedoms in this context while such efforts would reduce the risk of children being affected by the advertising industry negatively. It is noteworthy to recall that allowing children to exercise their right to privacy and data protection and ensuring that the data processing activities of a company do not disrespect children’s rights as individuals and that children are not discriminated in the sense that they are put in a secondary position in the context of ‘consent’, will also make sure that such practices are compliant with Article 36 of the Convention, which calls for children

80

81 For further considerations on children and privacy, see: United Nations Children’s Fund, ‘Privacy, Protection of Personal Information and Reputation’, Discussion Paper, UNICEF, Geneva, March 2017, available at ‘PRIVACY, PROTECTION OF PERSONAL INFORMATION AND REPUTATION’. cited in Gorostiaga and others (n 42). Page 23

82 Recital 40 GDPR. For consumer law, such special requirements regarding the form in which information is communicated to children are most likely to flow from Art. 3(3) of the Unfair Commercial Practices Directive, and here more specifically the provisions about vulnerable consumers. Cited in Natali Helberger, Frederik Zuiderveen Borgesius and Agustin Reyna, ‘The Perfect Match? A Closer Look at the Relationship Between EU Consumer Law and Data Protection Law’ (2017) 54 Common Market Law Review <https://www.ivir.nl/publicaties/download/CMLR_2017.pdf> accessed 2 March 2020. Page 9

83 “*The Guidance also recommends providing different versions of the privacy notice if the target audience covers a wide age range, even in cases where parental consent is triggered as the lawful basis. It is our understanding however that in cases where Article 8 applies the privacy notice must be directed to the holder of parental responsibility. It should be clarified that this suggestion should be considered as good practice that will help raise the level of protection to children and that it is not mandatory under the GDPR.*” ‘ISFE Response to the ICO Public Consultation On Children and the GDPR’ (n 30). Page 5

to be protected from all types of exploitation, including commercial exploitation.⁸⁴ Overall, in light of the above discussions, it can be concluded that Gamecell has gaps in their practices and definitely failures in implementation of the rules and laws under the applicable law for accountability purposes.

III. Children Privacy on the Ground: Responsibilities of Online Platforms

Children deserve specific protection when online gaming companies use their personal data for marketing purposes or creating personality or user profiles. In addition to drawing attention to the responsibilities of online platforms under the legislation, this Section provides guidance and suggests adoption of some efficient and children focused applications in practice. The UNCRC⁸⁵ recognises that children need special safeguards and care in all aspects of their life and requires that these should be guaranteed by appropriate legal protections. Accordingly, it should always be kept in mind that whatever decision online gaming companies are taking, if the processing of personal data involves children, then the primary and ultimate priority should be safeguard the best interests of the children. Online gaming companies should respect children's rights and freedoms and take steps to provide special safeguards by taking their needs and their vulnerability into account. The examples given in this Section aim to lead the way for online gaming companies, helping them in their efforts in compliance with the data protection laws in general independent of any specific applicable law. The below given examples provide a general understanding of the recent developments and good practices which should be internalised in any action or decision taken by the online gaming companies. By doing so, we aim to underscore the importance of the universality of data protection and protection of children, which should not be limited to any specific requirement prescribed by a particular law or regulation and therefore for which the standards should not depend on the country in which the online gaming company operates. If the essence lying at the heart of the approaches taken in the below given sub-sections are internalised then compliance with the relevant rules and regulations in any country would not only be easier, but would also contribute to the enhancement of children's rights globally. To provide this approach, this Section first starts with explaining the recently published Age Appropriate Design Code of Practice, then moves to PEGI and YouTube's current practices with regards to treatment of children's data and concludes by wrapping up the lessons learned for Gamecell for implementing the good practices which can set an example for them.

⁸⁴ Gorostiaga and others (n 42). Page 10

⁸⁵ 'OHCHR | Convention on the Rights of the Child' <<https://ohchr.org/EN/ProfessionalInterest/Pages/CRC.aspx>> accessed 2 March 2020.

The ICO's Age Appropriate Design: A Code of Practice for Online Services

In the UK, recently, the ICO took a concrete step towards protecting children online and published the Age Appropriate Design Code⁸⁶, a code of practice to protect children's privacy online and provided 15 standards that online services including online game platforms should meet in order to ensure that children's privacy is protected. These standards are expected of those responsible for designing, developing or providing online services such as online games, social media platforms, connected toys, and apps. In the context of online games, according to this Code, digital services are automatically required to provide children with a 'built-in' baseline of data protection when they download a game.⁸⁷ In other words, privacy settings of an online game platform should be set to high by default. Also, under this Code, the nudge techniques used by online game platforms should not be utilized to encourage children to weaken their settings.

In addition to the abovementioned requirements, with regards to location data settings, the Code provides that the data showing where a child is should not be collected and therefore the location settings should automatically be turned off by default without requiring a child to take a positive action, make an effort to switch off the location settings. Also, in line with the core principle of data minimisation provided under Article 5(1)(c) of the GDPR and the Data Protection Act ("DPA") 2018, data collection and sharing should be minimised, profiling which enables children to receive targeted content is required to be switched off by default. These rules are set for the ultimate purpose of safeguarding the best interests of the child which should be a primary and ultimate consideration in taking any step, for example, designing or developing an online game platform. In this context, the Code provides guidance on data protection safeguards that is directly applicable in practice, aiming to make sure that online services, in our context, online games are appropriate for children's usage. The 15 standards⁸⁸ are listed below and should be interpreted in the context of online gaming services for the purposes of this article and lead the way in their practices.

1 – **"Best interests of the child"**⁸⁹: As mentioned before, the Code values the best interests of the child and puts it as a primary consideration when designing and developing online services that are likely to be accessed by a child."

86 See Elizabeth Denham, 'Age Appropriate Design: A Code of Practice for Online Services | ICO' (ICO) <<https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/>> accessed 2 March 2020.

87 See ICO, 'ICO Publishes Code of Practice to Protect Children's Privacy Online | ICO' (2020) <<https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/01/ico-publishes-code-of-practice-to-protect-children-s-privacy-online/>> accessed 2 March 2020.

88 See ICO, 'Code Standards | ICO' <<https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/code-standards/>> accessed 2 March 2020.

89 See also recommendations in the context of COPPA where Livingstone suggests that a similar approach to be taken in to US. Eleonora Mazzoli and Sonia Livingstone, 'Problematic Data Practices and Children's Online Privacy: Reviewing the COPPA Rule | Media@LSE' (February 2020) <<https://blogs.lse.ac.uk/medialse/2020/02/04/problematic-data-practices-and-childrens-online-privacy-reviewing-the-coppa-rule/>> accessed 2 March 2020.

2 - **"Data protection impact assessments ("DPIA"):** The Code brings this standard and urges online service providers to assess and mitigate risks resulting from data processing activities, which may affect children's rights and freedoms and put them at risk. This standard further underscores the importance of taking different ages of children into account as well as considering capacities, development needs in order to ensure that the DPIA builds in compliance with this Code. It is noteworthy to state that this standard is also highly relevant for the purposes of Article 35 of the GDPR."

3 - **"Age appropriate application:** This standard underlines taking a risk-based approach to recognise users' age and ensuring that the standards set out under this Code are applied to child users effectively. This standard further elaborates by giving two options. The first one is establishing users' age with a level of certainty that is appropriate to the risks to the rights and freedoms of children that arising from online services' data processing activities. Alternatively, the second option provided under this standard is to apply all the standards provided in this Code to all the users."

4 - **"Transparency:** This standard ensures that the community standards, any published terms, policies and the privacy information online services give to users are concise, prominent and unambiguously written with a clear language that is appropriate to the age of the child. Furthermore, this standard urges online services to provide additional specific 'bite-sized' explanations about how users' personal data is used when that use is activated."

5 - **"Detrimental use of data:** Aligned with the first standard, this standard urges online services not to use children's personal data in ways that have been shown to be detrimental to their wellbeing, or that go against industry codes of practice, other regulatory provisions or Government advice."

6 - **"Policies and community standards:** This standard aims to ensure that online service companies uphold their own published terms, policies and community standards such as privacy and content policies."

7 - **"Default settings:** The Code ensures that the standard for settings is 'high privacy' by default except in very limited circumstances where the best interests of the child is made priority and the company is required to demonstrate a compelling reason for a different default setting."

8 - **"Data minimisation:** This standard basically ensures that data collection and retainment is limited to the minimum amount of personal data the company needs to provide the elements of its service in which a child is actively and knowingly engaged. This standard further provides that children separate should be given different choices over which elements they wish to activate."

9 – “**Data sharing:** This standard requires companies not to disclose children’s data unless there is a compelling reason that can be demonstrated in light of the best interests of the child.”

10 – “**Geolocation:** Unless there is a compelling reason that can be demonstrated, taking into account the first standard, namely, the best interests of the child, the Code urges companies to switch geolocation options off by default. In addition, this standard requires companies to provide a clear sign for children when location tracking is active and adds that options that make children’s visible to others must default back to ‘off’ at the end of each particular session.”

11 – “**Parental controls:** This standard aims to ensure that children are given age appropriate information about the parental controls the company provides. Similarly, it requires online services to show an obvious sign to children when they are monitored, if parents or carers are provided with the option to monitor their child’s online activity or track their location. This standard is important not only for children’s protection, but also for the relationship that is built on trust and transparency between the parents and their children.”

12 – “**Profiling:** Unless there is a compelling reason that can be demonstrated, taking into account the first standard, namely, the best interests of the child, this standard urges online services to switch options that use profiling off by default. Furthermore, this standard aims to ensure that online services allow profiling only if the appropriate measures are in place in order to protect children from any harmful effects such as being fed content that is detrimental to their health or wellbeing.”

13 – “**Nudge techniques:** This standard requires online services not to use nudge techniques to lead or in any way encourage children to turn off their privacy protections, to provide unnecessary personal data or weaken their protection in any possible way.”

14 – “**Connected toys and devices:** If an online service provides a connected toy or device, this standard urges the company to ensure it includes effective tools and takes the necessary measures to enable conformance to this Code.”

15 – “**Online tools:** The last standard of the Code asks online services to provide prominent and accessible tools in order to help children exercise their right to data protection and report concerns.”

One of the main problems that is aimed to be addressed in this Code is the fact that the Internet was not built for children.⁹⁰ Similar to the laws that exist in the offline environments, there should be laws and regulations that set rules to ensure

90 See ICO, ‘ICO Publishes Code of Practice to Protect Children’s Privacy Online | ICO’ (n 87).

that our children are protected online environments as well. Internalising the above mentioned standards are crucial for GDPR compliance reasons as well. This is because age appropriate design and protecting children from companies' exploitation of their data is strongly linked with the notion of fairness provided under Article 5(1) (a) of the GDPR. This Code provides practical measures and safeguards to ensure processing under the GDPR can be considered 'fair' in the context of online risks to children, and will help companies comply with the following provisions: Article 5(1) (a): the fairness, lawfulness and transparency principle; Article 5(1)(b): the purpose limitation principle; Article 5(1)(c): the data minimisation principle; Article 5(1)(e): the storage limitation principle; Article 5(2): the accountability principle; Article 6: lawfulness of processing; Articles 12, 13 and 14: the right to be informed; Articles 15 to 20: the rights of data subjects; Article 22: profiling and automated decision-making; Article 25: data protection by design and by default; and Article 35: DPIAs. Although this Code was not an obligation under the GDPR, it is a fact that it provided solid standards that would help companies in their compliance with the relevant rules touching children's lives under the GDPR. The approach taken in this Code and the priority of 'best interests of the child' should set an example not only for the online gaming companies, but also for the DPAs globally.

PEGI

For online gaming companies, another recommendation can be to truly understand and internalise PEGI, which can be a great example that is recognised throughout Europe and is used with the support of the European Commission; PEGI is considered as a model of European harmonisation in the field of the protection of children.⁹¹ It uses age ratings which can be described as the systems used to make sure that entertainment content, including games or mobile apps, is clearly labelled with a minimum age recommendation based on the content they have. This system helps users and parents to make informed decisions by providing guidance to them particularly in order to help them decide whether or not to buy a particular product for a child.⁹² PEGI also values parental control tools that are beneficial for all members of a family since they enable parents to safeguard their children's privacy, their protection and online safety according to various parameters. PEGI allows parents to select the games that children can play (based on the PEGI age ratings), limit and monitor their online spending while allowing parents to control access to internet browsing, chat and the amount of time their children spend playing games.⁹³ Although most games are generally suitable for individuals of all ages, some games are only suitable for older children, some for adults and others are for younger children.

91 'Pegi Age Ratings | Gaming Nerds' <<https://www.gamingnerds.co.uk/pegi-age-ratings>> accessed 2 March 2020.

92 See 'PEGI Age Ratings | Pegi Public Site' <<https://pegi.info/page/pegi-age-ratings>> accessed 2 March 2020.

93 See 'Parental Control Tools | Pegi Public Site' <<https://pegi.info/index.php/parental-controls>> accessed 2 March 2020.

The PEGI rating addresses this difference of suitability for different ages and considers the age suitability of a game. It is noteworthy to mention that PEGI's age suitability does not consider the level of difficulty in terms of 'suitability' of a game for a specific age. For example, a PEGI 3 game can be considerably difficult to master for young children, however it would not contain any inappropriate content. On the other hand, PEGI 18 games can be very easy to play, however, they may have inappropriate elements for younger children.

It is noteworthy to state that "Güvenli Oyna"⁹⁴ draws attention to the PEGI labels on its website by putting the mini versions of PEGI rates on both sides of the page. These labels which show PEGI rates do not disappear when one navigates on the website. It is clear that such rating is expected from online game platforms to be used as a minimum standard. Using PEGI labels would not only help parents, protect children but also would help companies to demonstrate their efforts for compliance with Article 5(1)(a) and therefore contributing to their obligations in terms of accountability. PEGI is regarded as a model of European harmonisation in the field of child protection.⁹⁵ Adopting such an approach in every country the company operates would also contribute to the idea that protecting children in the online ecosystem is a global concern. It is important to note that failure to comply with rules set out in the Code of Conduct can give rise to sanctions.⁹⁶ The above given content descriptors are of use for labels are black and white icons that are illustrations in a way depicting the content of the game with black and white figures.⁹⁷ These content descriptors require the game provider to check the set age rules for the content in question and therefore in a way puts responsibility on it with regards to the target audience. Although there was disagreement when deciding the symbols that are used in the content descriptors⁹⁸, in the end the current figures and symbols seem to appeal to children residing in different countries. Therefore, it is suggested for companies to stick to recognised and acceptable symbols and figures as in PEGI, which would also promote and support a harmonized language globally.

YouTube and YouTube Kids Before and After FTC Decision

In November 2019, YouTube announced its plan to have creators label any videos of theirs that may appeal to children. As from January 2020, if a content creator marks its content to be targeted to children, then it should act accordingly in order to comply

94 'TİCARİ İLETİŞİM VE TİCARİ ELEKTRONİK İLETİLER HAKKINDA YÖNETMELİK' (n 77).

95 Children in the Online World: Risk, Regulation, Rights By Elisabeth Staksrud page 102, 103

96 See 'The PEGI Code of Conduct | Pegi Public Site' <<https://pegi.info/pegi-code-of-conduct>> accessed 26 February 2020.

97 'What Do the Labels Mean? | Pegi Public Site' <<https://pegi.info/what-do-the-labels-mean>> accessed 26 February 2020.

98 'Children in the Online World: Risk, Regulation, Rights - Elisabeth Staksrud - Google Books' <https://books.google.co.uk/books?id=TWs3DAAAQBAJ&pg=PT114&lpg=PT114&dq=PEGI+considered+as+a+model+of+European+harmonisation+in+the+field+of+the+protection+of+children&source=bl&ots=B6fqeDE_JM&sig=ACfU3U0LpZUMYL-0palrr5pL.KOGtFuKMPQ&hl=en&sa=X&ved=2ahUKEwjg> accessed 26 February 2020. Page 102

with the rules and laws applicable in the data protection regime. Thus, YouTube made changes in their data collection and usage activities involving children. To elaborate, the recent changes involve YouTube's data processing activities relating to children's content on YouTube.com. These changes address concerns raised by the US Federal Trade Commission (FTC) regarding the company's compliance under the COPPA. As a result of these concerns, the changes made by YouTube requires a creator to inform YouTube if the content is made for children. Furthermore, YouTube announced that it will use machine learning which will help to identify videos that clearly target children or young audiences.⁹⁹ Following the FTC's decision in 2019, it was decided that all creators should be required to designate their content as made for kids or not made for kids in YouTube Studio.¹⁰⁰ Accordingly, as a rule, data from anyone watching the content which is designated as made for children will be treated as coming from a child, regardless of the age of the user.¹⁰¹ On its recent post on YouTube official blog dated January 6, 2020, it was underscored that a video is made for kids if it is intended for kids, taking into consideration a variety of factors. These factors include the subject matter of the video, whether the video has an emphasis on kids characters, themes, toys or games, and more."¹⁰² Also, it was announced that Another important change concerns personalised ads, YouTube announced that its practices involving delivering ads to children will be compliant with the rules under the COPPA. This means that it will no longer serve personalised ads (ads that are targeted to users based on their past usage of Google products and services) to child audiences. However, it also added that YouTube will continue to serve non-personalised ads (ads that are shown based on context rather than on user data) on content that is made for kids. Moreover, some features such as comments will no longer be available on the content that is made for children. Similarly, the ability to comment will no longer be available on the watch page and likes/dislikes as well as subscriptions on this content will not appear on public lists. Overall, to be able to protect children , viewers will have minimum engagement options with 'made for kids' content on YouTube.com.¹⁰³

99 See 'Upcoming Changes to Children's Content on YouTube.Com - YouTube Help' <<https://support.google.com/youtube/answer/9383587?hl=en-GB>> accessed 26 February 2020.

100 See 'Official YouTube Blog: Better Protecting Kids' Privacy on YouTube' <<https://youtube.googleblog.com/2020/01/better-protecting-kids-privacy-on-YouTube.html>> accessed 26 February 2020.

101 See 'Google and YouTube Will Pay Record \$170 Million for Alleged Violations of Children's Privacy Law | Federal Trade Commission' (n 61). and 'YouTube's COPPA Changes Begin Today, Possibly Affecting Creator Revenue - Search Engine Journal' <<https://www.searchenginejournal.com/youtubes-coppa-changes-begin-today-possibly-affecting-creator-revenue/342433/#close>> accessed 26 February 2020.

102 'Official YouTube Blog: Better Protecting Kids' Privacy on YouTube' (n 100).; See also 'YouTube Channel Owners: Is Your Content Directed to Children? | Page 27 | Federal Trade Commission' <<https://www.ftc.gov/news-events/blogs/business-blog/2019/11/youtube-channel-owners-your-content-directed-children?page=26>> accessed 26 February 2020.

103 'Upcoming Changes to Kids Content on YouTube.Com - YouTube Help' <<https://support.google.com/youtube/answer/9383587?hl=en>> accessed 26 February 2020.; See also 'YouTube Channel Owners: Is Your Content Directed to Children? | Federal Trade Commission' <<https://www.ftc.gov/news-events/blogs/business-blog/2019/11/youtube-channel-owners-your-content-directed-children>> accessed 26 February 2020.

Lessons Learned for Gamecell

The ICO's suggestions as to the legal basis to process children's data can be helpful for online gaming companies including Gamecell. Firstly, if the company is going to rely on consent to process children's data, then it should be as transparent and as clear as possible to ensure that children can comprehend what they are consenting to.¹⁰⁴ Also, as discussed above in Section I, companies should make sure that they do not exploit any imbalance of power in the relationship between us. In Gamecell's case, it is clear that Gamecell bundles consent in certain provisions and in a way that leaves no choice to data subjects but to agree or not to use its services. This is an example for abuse of the imbalance of powers which is a self-destruction method for the obtained consent, deeming it invalid. Therefore, it can be concluded that the consent obtained in the above mentioned provisions in Section II can be seen as invalid for the reasons explained in the above Sections. Secondly, if a company chooses to rely on 'necessary for the performance of a contract'; the company should carefully consider the children's competence to comprehend what they are agreeing to, and to enter into a contract and create legal relations. Lastly, if the company opts to rely upon 'legitimate interests', it should take responsibility for identifying the risks and consequences of the processing, and put age appropriate safeguards in place. As stated before, unfortunately, the processing of children's personal data carried out by Gamecell does not meet the requirements set out under the GDPR, nor the check list given by the ICO.¹⁰⁵ It is a no brainer to say that the standards established in the ICO's Age Appropriate Design Code deserve careful consideration. Especially, for transparency and fairness purposes, as discussed above, there is a need to use child friendly language¹⁰⁶ also for compliance with Article 12(1) and Article 5(1)(a) and therefore Article 5(2) purposes. Gamecell lacks this approach and the approach taken in the above summarised recent developments cannot be seen in their terms and policies. With regard to Privacy Policies, it is crucial that the above explained standards of the Age Appropriate Code are taken into account and privacy notices are clear, and unlike Gamecell's policies, the privacy notices should be presented in plain, age-appropriate language. It is also crucial that the companies use child friendly ways of presenting privacy information. Some examples can be diagrams, cartoons, graphics, icons and symbols as used in PEGI examples.¹⁰⁷ Using clear language or icons, symbols etc. would not only help companies to comply with the relevant rules set out under data protection law for accountability reasons, but also satisfy the expectations derived from the

¹⁰⁴ See 'Children | ICO' (n 10).

¹⁰⁵ See *ibid*.

¹⁰⁶ See for example 'UN Convention on the Rights of the Child in Child Friendly Language' <<https://static.unicef.org/rightsite/files/uncrcchildfriendlylanguage.pdf>> accessed 26 February 2020.

¹⁰⁷ Another example can be just in time notices; See also 'ICO Endorses Use of "Just-in-Time" Notices' <<https://iapp.org/news/a/ico-endorses-use-of-just-in-time-notices/>> accessed 26 February 2020.

absolute need to respect children's freewill and their capacity by recognising them as data subject. This can be done by being transparent and for example explaining why the company requires the personal data that is asked for, and for what purposes this data will be used for, in a way which is reasonably expected for a child to understand. As the ICO notes down, as a matter of good practice, there is a need to make clear the risks inherent in the processing, and how the company intends to prevent them or protect children against them.¹⁰⁸ This explanation should be made in a child friendly way, so that children and their parents comprehend the implications of sharing their personal data.¹⁰⁹ In addition to these, the companies should inform children about their rights¹¹⁰, again in a clear, plain, and child friendly language. When Gamecell's terms and policies are examined, these efforts seem to be lacking in the wording they used or even for some provisions there were contradicting statements with the above discussed approach. Therefore, it is highly recommended for different stakeholders of the online gaming ecosystem including online gaming companies to employ the reasoning, purposes adopted in PEGI, Age Appropriate Design Code as well as the YouTube's recent changes in its practices to safeguard children and also help parents build trust in the system, in a way, by sharing their burden to make sure that their children and their rights are protected online. The comments provided in Section II should be re-considered in light of the above given examples and recent developments summarised in this Section in order to grasp a better understanding of the needs of children and to be able to keep up with practical trends prioritized to achieve a fair application of the laws and rules for the best interest of the children globally.

Conclusion

Online games and the usage of the Internet are now omnipresent and deeply ingrained in the lives of children. From widespread engagement with the Internet through mobile devices, search engines, laptops social media to interactive TVs, children and parents are now faced with a plethora of new challenges and risks for which they need protection. Currently, there is a gap that exists among the essences lying at the heart of fundamental rights to privacy and data protection, other fundamental rights protected by international instruments concerning children, the legal and practical implications of the rules relating to 'consent' as well as 'fairness'. Lack of practical guidance explaining how to implement the rules under the data protection laws is not an excuse for online gaming companies since the best interests of children is beyond obvious to us all. Although there may be challenges in applying the above mentioned

108 See 'Children | ICO' <<https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/children/?q=privacy+noticeshttps%3A%2F%2Fico.org.uk%2Ffor-organisations%2Fguide-to-the-general-data-protection-regulation-gdpr%2Findividual-rights%2Fright-to-be-infor>> accessed 26 February 2020.

109 *ibid.*

110 See also *ibid.*

rules in general, these challenges and some minor gaps possibly existing due to clarity of the laws and rules should have only be limited to minor details in companies' terms and policies. However, Gamecell's unacceptable practices that can be seen in the statements chosen in Section II are intolerable and by no means acceptable practices. Therefore, this article urges all the stakeholders of the online gaming ecosystem to take the necessary steps for accountability reasons, truly understand the rules set out in the applicable legal framework, and most importantly, remember that the users are individuals whose rights and freedoms are non-negotiable. It is therefore imperative that stakeholders of the online gaming ecosystem to acquire a detailed understanding of the importance of children's online privacy and the challenges that are relevant in today's digital age in order to take necessary measures to protect children and respect their rights. Even though the issues rotating around data protection and privacy have become soaring topics in recent years, it is still obvious that unacceptable practices exist in real life. Finally, it is critical to underscore the importance of "fairness" and remind online gaming companies that it should be central to all your processing of children's personal data.

Hakem Değerlendirmesi: Dış bağımsız.

Çıkar Çatışması: Yazarlar çıkar çatışması bildirmemiştir.

Finansal Destek: Yazarlar bu çalışma için finansal destek almadığını beyan etmiştir.

Peer-review: Externally peer-reviewed.

Conflict of Interest: The authors have no conflict of interest to declare.

Financial Disclosure: The authors declared that this study has received no financial support.

Bibliography

- '2019 Year In Review — SuperData, a Nielsen Company' <<https://www.superdataresearch.com/2019-year-in-review>> accessed 24 February 2020
- 'AÇIK RIZA' <<https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/66b2e9c4-223a-4230-b745-568f096fd7de.pdf>> accessed 26 February 2020
- Article29, 'ARTICLE29 Newsroom - Guidelines on Transparency under Regulation 2016/679 (Wp260rev.01) - European Commission' <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227> accessed 24 February 2020
- Article 29 Working Group, 'ARTICLE29 Newsroom - Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679 (Wp251rev.01) - European Commission' (2018) <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053> accessed 24 February 2020
- Bird&Bird, 'Principles | Children' <https://www.twobirds.com/~/_/media/pdfs/gdpr-pdfs/24--guide-to-the-gdpr--children.pdf?la=en> accessed 24 February 2020
- BrandimarteL,AcquistiAandLoewensteinG, 'Misplaced Confidences' (2013)4 Social Psychological and Personality Science 340 <<http://journals.sagepub.com/doi/10.1177/1948550612455931>> accessed 24 February 2020

- ‘CHILDREN’S ONLINE PRIVACY AND FREEDOM OF EXPRESSION’ <[https://www.unicef.org/csr/files/UNICEF_Childrens_Online_Privacy_and_Freedom_of_Expression\(1\).pdf](https://www.unicef.org/csr/files/UNICEF_Childrens_Online_Privacy_and_Freedom_of_Expression(1).pdf)> accessed 18 February 2020
- ‘Children | ICO’ <<https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/children/>> accessed 24 February 2020
- ICO <<https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/children/?q=privacy+noticeshttps%3A%2F%2Fico.org.uk%2Ffor-organisations%2Fguide-to-the-general-data-protection-regulation-gdpr%2Findividual-rights%2Fright-to-be-infor>> accessed 26 February 2020
- ‘Children in the Online World: Risk, Regulation, Rights - Elisabeth Staksrud - Google Books’ <https://books.google.co.uk/books?id=TWs3DAAAQBAJ&pg=PT114&lpg=PT114&dq=PEGI+considered+as+a+model+of+European+harmonisation+in+the+field+of+the+protection+of+children&source=bl&ots=B6fqeDE_JM&sig=ACfU3U0LpZUMYL0palr5pLK-gOGtFuKMPQ&hl=en&sa=X&ved=2ahUKEwjg> accessed 26 February 2020
- ‘Consent | ICO’ <<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/>> accessed 26 February 2020
- ‘Consent on the Internet Means “Opting-in” in Europe’ (2019) <www.hoganlovells.com> accessed 26 February 2020
- ‘Contribution from the Multistakeholder Expert Group to the Stock-Taking Exercise of June 2019 on One Year of the GDPR Application’ (2019) <<http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3537&NewSearch>> accessed 24 February 2020
- ‘Cookies, the GDPR, and the EPrivacy Directive - GDPR.Eu’ <<https://gdpr.eu/cookies/>> accessed 26 February 2020
- ‘Creating a Better Internet for Kids | Shaping Europe’s Digital Future’ <<https://ec.europa.eu/digital-single-market/en/policies/better-internet-kids>> accessed 24 February 2020
- Denham E, ‘Age Appropriate Design: A Code of Practice for Online Services | ICO’ (*ICO*) <<https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/>> accessed 2 March 2020
- EDPB, ‘Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3)-Version for Public Consultation’ (2018) <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_en.pdf> accessed 24 February 2020
- EDPB, ‘Guidelines 2/2019 on the Processing of Personal Data under Article 6(1)(b) GDPR in the Context of the Provision of Online Services to Data Subjects Adopted-Version for Public Consultation’ (2019) <https://edpb.europa.eu/sites/edpb/files/consultation/edpb_draft_guidelines-art_6-1-b-final_public_consultation_version_en.pdf> accessed 24 February 2020
- ‘ELEKTRONİK HABERLEŞME KANUNU 5809’ (2008) <<https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5809.pdf>> accessed 26 February 2020
- ‘European E-Justice Portal - Unfair Contract Terms Directive (93/13)’ <https://e-justice.europa.eu/content_unfair_contract_terms_directive_9313-627-en.do> accessed 24 February 2020
- ‘Examples of Processing “Likely to Result in High Risk” | ICO’ <<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/examples-of-processing-likely-to-result-in-high-risk/>> accessed 26 February 2020

- “Fortnite” May Be a Virtual Game, but It’s Having Real-Life, Dangerous Effects - The Boston Globe’ <https://www.bostonglobe.com/metro/2019/03/31/unexplained-weight-loss-children-boston-nutritionist-makes-her-diagnosis-fortnite/eNMmGkK814IOsCwDDk2ZPN/story.html?s_campaign=8315> accessed 26 February 2020
- ‘Gamecell - Oyunlar. Arkadaşlar. Eğlence.’ <<https://www.gamecell.com/tr/userAgreement.html>> accessed 26 February 2020
- <<https://www.gamecell.com/tr/privacyPolicy.html>> accessed 26 February 2020
- ‘Gaming the System | Children’s Commissioner for England’ <<https://www.childrenscommissioner.gov.uk/publication/gaming-the-system/>> accessed 26 February 2020
- ‘GDPR Implementation In Respect of Children’s Data and Consent Centre for Information Policy Leadership 6 March 2018 2 CIPL’s TOP TEN MESSAGES ON GDPR IMPLEMENTATION IN RESPECT OF CHILDREN’S DATA’ (2018) <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_-_gdpr_implementation_in_respect_of_childrens_data_and_consent.pdf> accessed 24 February 2020
- ‘Google and YouTube Will Pay Record \$170 Million for Alleged Violations of Children’s Privacy Law | Federal Trade Commission’ <<https://www.ftc.gov/news-events/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations>> accessed 26 February 2020
- ‘Google Is Fined \$170 Million for Violating Children’s Privacy on YouTube - The New York Times’ <<https://www.nytimes.com/2019/09/04/technology/google-youtube-fine-ftc.html>> accessed 26 February 2020
- Gorostiaga A and others, ‘Child Rights and Online Gaming: Opportunities & Challenges for Children and the Industry’ (2019) <https://www.unicef-irc.org/files/upload/documents/UNICEF_CRBDigitalWorldSeriesOnline_Gaming.pdf> accessed 18 February 2020
- Healthline, ‘What Science Says About Video Games and ADHD’ <<https://www.healthline.com/health-news/the-link-between-adhd-and-video-games>> accessed 24 February 2020
- Helberger N, Zuiderveen Borgesius F and Reyna A, ‘The Perfect Match? A Closer Look at the Relationship Between EU Consumer Law and Data Protection Law’ (2017) 54 Common Market Law Review <https://www.ivir.nl/publicaties/download/CMLR_2017.pdf> accessed 2 March 2020
- , ‘THE PERFECT MATCH? A CLOSER LOOK AT THE RELATIONSHIP BETWEEN EU CONSUMER LAW AND DATA PROTECTION LAW’ (2017) 54 Common Market Law Review <https://www.ivir.nl/publicaties/download/CMLR_2017.pdf> accessed 24 February 2020
- ICO, ‘Code Standards | ICO’ <<https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/code-standards/>> accessed 2 March 2020
- , ‘The General Data Protection Regulation Children and the GDPR’ (2018) <<https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr-1-0.pdf>> accessed 24 February 2020
- , ‘ICO Publishes Code of Practice to Protect Children’s Privacy Online | ICO’ (2020) <<https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/01/ico-publishes-code-of-practice-to-protect-children-s-privacy-online/>> accessed 2 March 2020
- ‘ICO Endorses Use of “Just-in-Time” Notices’ <<https://iapp.org/news/a/ico-endorses-use-of-just-in-time-notice/>> accessed 26 February 2020

- Information Commissioners Office, 'How Does the Right to Be Informed Apply to Children?' (2018) <<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr/how-does-the-right-to-be-informed-apply-to-children/>> accessed 18 February 2020
- Ingrida Milkaite and Eva Lievens, 'Better Internet for Kids - Status Quo Regarding the Child's Article 8 GDPR Age of Consent for Data Processing across the EU' (2019) <<https://www.betterinternetforkids.eu/web/portal/practice/awareness/detail?articleId=3017751>> accessed 18 February 2020
- 'Internet and Video Game Addictions: A Cognitive Behavioral Approach' <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0101-60832014000300082> accessed 24 February 2020
- 'ISFE Response to the ICO Public Consultation On Children and the GDPR' (2018) <www.isfe.eu> accessed 24 February 2020
- Kardefelt-Winther D, 'How Does the Time Children Spend Using Digital Technology Impact Their Mental Well-Being, Social Relationships and Physical Activity? An Evidence-Focused Literature Review. I How Does the Time Children Spend Using Digital Technology Impact Their Mental We' (2017) <www.unicef-irc.org> accessed 24 February 2020
- 'Kids and Smartphones and Video Game Addiction - Consumer Reports' <<https://www.consumerreports.org/gaming/kids-glued-to-smartphones-video-games-could-signal-addiction/>> accessed 26 February 2020
- Livingstone S, 'Children: A Special Case for Privacy? Article (Published Version) (Refereed)' (2018) <http://eprints.lse.ac.uk/89706/1/Livingstone_Children-a-special-case-for-privacy_Published.pdf> accessed 24 February 2020
- Macenaite M and Kosta E, 'Consent for Processing Children's Personal Data in the EU: Following in US Footsteps?' (2017) 26 Information and Communications Technology Law 146
- Mazzoli E and Livingstone S, 'Problematic Data Practices and Children's Online Privacy: Reviewing the COPPA Rule | Media@LSE' (February 2020) <<https://blogs.lse.ac.uk/medialse/2020/02/04/problematic-data-practices-and-childrens-online-privacy-reviewing-the-coppa-rule/>> accessed 2 March 2020
- 'Media Moment: So Your Child Wants To Go To A Video Game Convention | Center on Media and Child Health' <<https://cmch.tv/media-moment-so-your-child-wants-to-go-to-a-video-game-convention/>> accessed 26 February 2020
- 'Official YouTube Blog: Better Protecting Kids' Privacy on YouTube' <<https://youtube.googleblog.com/2020/01/better-protecting-kids-privacy-on-YouTube.html>> accessed 26 February 2020
- 'OHCHR | Convention on the Rights of the Child' <<https://ohchr.org/EN/ProfessionalInterest/Pages/CRC.aspx>> accessed 2 March 2020
- 'Online Games | NSPCC' <<https://www.nspcc.org.uk/keeping-children-safe/online-safety/online-games/>> accessed 26 February 2020
- 'Online Gaming | Childline' <<https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/online-gaming/>> accessed 26 February 2020
- 'Parental Control Tools | Pegi Public Site' <<https://pegi.info/index.php/parental-controls>> accessed 2 March 2020
- 'Pegi Age Ratings | Gaming Nerds' <<https://www.gamingnerds.co.uk/pegi-age-ratings>> accessed 2 March 2020

- 'PEGI Age Ratings | Pegi Public Site' <<https://pegi.info/page/pegi-age-ratings>> accessed 2 March 2020
- 'PRIVACY, PROTECTION OF PERSONAL INFORMATION AND REPUTATION'
- 'Privacy and Electronic Communications Regulations Guidance on the Rules on Use of Cookies and Similar Technologies Contents'
- 'Processing of Personal Data General Principles'
- Raynes-Goldie K and Allen M, 'Gaming Privacy: A Canadian Case Study of a Co-Created Privacy Literacy Game for Children' <<http://pdfs.semanticscholar.org/1e30/e92594e9728148b5438be71e51943d0ae9c4.pdf>> accessed 24 February 2020
- 'Right of Access | ICO' <<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/>> accessed 24 February 2020
- 'Study on the Impact of Marketing through Social Media, Online Games and Mobile Applications on Children's Behaviour | European Commission' (2016) <https://ec.europa.eu/info/publications/study-impact-marketing-through-social-media-online-games-and-mobile-applications-childrens-behaviour_en> accessed 24 February 2020
- 'The Games Industry Shouldn't Be Ripping off Children | Geraldine Bedell | Opinion | The Guardian' <<https://www.theguardian.com/commentisfree/2019/sep/15/games-industry-shouldnt-be-ripping-of-children>> accessed 26 February 2020
- 'The Keys to Data Protection A Guide for Policy Engagement on Data Protection' (2018) <<https://privacyinternational.org/sites/default/files/2018-09/Data Protection COMPLETE.pdf>> accessed 24 February 2020
- 'The PEGI Code of Conduct | Pegi Public Site' <<https://pegi.info/pegi-code-of-conduct>> accessed 26 February 2020
- 'TİCARİ İLETİŞİM VE TİCARİ ELEKTRONİK İLETİLER HAKKINDA YÖNETMELİK' (*Resmî Gazete Sayısı: 29417*, 2015) <<https://www.mevzuat.gov.tr/Metin.Aspx?MevzuatKod=7.5.20914&MevzuatIliski=0>> accessed 26 February 2020
- 'UN Convention on the Rights of the Child in Child Friendly Language' <<https://static.unicef.org/rightsite/files/uncrcchildfriendlylanguage.pdf>> accessed 26 February 2020
- UNODC, 'The Use of Internet for Terrorist Purposes' (2012)
- 'Upcoming Changes to Children's Content on YouTube.Com - YouTube Help' <<https://support.google.com/youtube/answer/9383587?hl=en-GB>> accessed 26 February 2020
- 'Upcoming Changes to Kids Content on YouTube.Com - YouTube Help' <<https://support.google.com/youtube/answer/9383587?hl=en>> accessed 26 February 2020
- 'What Are the Rules on Cookies and Similar Technologies? | ICO' <<https://ico.org.uk/for-organisations/guide-to-pectr/guidance-on-the-use-of-cookies-and-similar-technologies/what-are-the-rules-on-cookies-and-similar-technologies/>> accessed 26 February 2020
- 'What Do the Labels Mean? | Pegi Public Site' <<https://pegi.info/what-do-the-labels-mean>> accessed 26 February 2020
- 'What Should Our General Approach to Processing Children's Personal Data Be? | ICO' <<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr/what-should-our-general-approach-to-processing-children-s-personal-data-be/>> accessed 26 February 2020

- 'WHO Gaming Addiction Classification [Video]' <<https://finance.yahoo.com/news/world-health-organizations-new-classification-video-game-addiction-good-thing-220236312.html>> accessed 26 February 2020
- 'YouTube's COPPA Changes Begin Today, Possibly Affecting Creator Revenue - Search Engine Journal' <<https://www.searchenginejournal.com/youtubes-coppa-changes-begin-today-possibly-affecting-creator-revenue/342433/#close>> accessed 26 February 2020
- 'YouTube Channel Owners: Is Your Content Directed to Children? | Federal Trade Commission' <<https://www.ftc.gov/news-events/blogs/business-blog/2019/11/youtube-channel-owners-your-content-directed-children>> accessed 26 February 2020
- 'YouTube Channel Owners: Is Your Content Directed to Children? | Page 27 | Federal Trade Commission' <<https://www.ftc.gov/news-events/blogs/business-blog/2019/11/youtube-channel-owners-your-content-directed-children?page=26>> accessed 26 February 2020

