Center for Open Access in Science ▪ https://www.centerprode.com/ojls.html
Open Journal for Legal Studies, 2022, *5*(1), 1-10.
ISSN (Online) 2620-0619 ▪ https://doi.org/10.32591/coas.ojls.0501.01001s

Legal Issues of Children's Personal Data Protection

Daria Smyr & Ekaterina Ulianova

Belarussian State University, Law Faculty, Minsk, REPUBLIC OF BELARUS

Received: 14 March 2022 ▪ Revised: 28 May 2022 ▪ Accepted: 15 June 2022

Abstract

The article deals with the problems of protecting the information privacy of minors in the online gaming sector. The authors analyze core approaches and methods of collection and processing of minors' personal data, special regulation of data processing of children's audience in light of some private company's experience, current liability practices, and also offers a set of legislative measures to improve the effectiveness of children's data protection both at the international and national level, measures for implementation of data subject rights.

Keywords: personal data protection, minors, gaming industry, consent to processing, minimization.

1. Introduction

The growing threat to the protection of the information privacy of children and minors in the game industry is gradually expanding its borders, together with the problem of tightened legislative requirements for companies to maintain their personal data still remains relevant.

The aim of the article is to analyse the legal regulation of the protection of personal data of minors and different methods of collecting and processing such data both on a national and international level.

This article is an evaluating study of minors' personal data protection as a whole. In view of the fact that the legal capacity of a child in an online environment remains an under-researched topic, the study aims at systematically describing the characteristics of children's rights and legal guarantees related to collecting and processing of their personal data. A qualitative approach and descriptive data by gathering observations without intervening were followed in this study.

In our view this is the most suitable approach to answering the research questions considering the legal orientation of the issue and diversity in national personal data regulation. No ethical considerations were involved in the choice of the information gathered.

The article is based on the comparative overview of data protection legislation. The research is grounded on dialectical, formal logical methods, methods of synthesis and analysis, comparative legal methods.

Correspondence: Daria Smyr, Belarussian State University, Law Faculty, Minsk, REPUBLIC OF BELARUS. E-mail: dasha.smyr@gmail.com.

- In recent years countries have adopted data protection laws with special requirements for collection and processing of personal data.
- Children's personal data should be afforded special protection by legislative and GameDev companies' measures by design and by default.
- Determining the optimal way to balance children's rights and the commercial benefits pose a lot of difficulties for business operation in different jurisdictions with unsimilar legislative approaches.
- The evidence from this study points out that governments with GameDev companies' collaboration should define the age limit for minor data subjects, the requirements for granting minors access to gaming services, develop and provide clear recommendations for data controllers on the processing of minors' data, promote and use international certification procedures for online platforms and services aimed at children's audience.

2. Discussion

In 2016, the EU adopted the General Data Protection Regulation (hereunder – GDPR). According to Preamble 38 to the GDPR, "children merit specific protection with regard to their personal data" due to their insufficient physical and psychological maturity, falling into the category of "vulnerable persons" who often have no recourse. For this, in order to prevent children from spreading their personal information, a number of additional obligations and restrictions were imposed on the controllers prior to the provisions of Article 8 of the GDPR. As said in paragraph 127 of the Guidelines 05/2020 on consent under Regulation 2016/6791, provisions of Article 8 of the GDPR are applicable to a limited number of situations where the following conditions are met.

Firstly, the processing of personal data is related to the offer of *information society services* directly to the child. As said in Explanations of the European Court of 2 December 2010 for case C-108/09, (Ker-Optika), it is explained that the scope of the term "information society service" includes a variety of services carried out and transferred online.

Secondly, Article 6(1)(a) and Article 7 of the GDPR confirm that lawful processing is ensured by the data subject's consent to the extent that "the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data".

Accordingly, the scope of Article 8 of the GDPR applies across sectors of the GameDev industry to companies of all sizes that offer online gaming services for the category of minors in the EU.

Probably the key factors for considering whether a particular service is subject to regulation are the likelihood of being attracted to the content of the service and the way the user can access the service. For this, the term "apply directly to a child" can be interpreted broadly, expanding its scope beyond businesses targeted to children, i.e., it can include services which have more than 50% possibility to be accessed by children.

Accordingly, for GDPR compliance, children's consent and parental responsibility are mandatory to be provided from the standpoint of technical processes of these services.

Now, whilst the GDPR does allow EU Member States to enact specific laws that deviate from the GDPR in several areas, most of the acts at the EU national level re-affirm the obligations regarding special regulation of the collection and processing of children's personal data.

As an example, for Irish policy makers and regulators, protection of children's personal data has become a priority target in recent years. With respect to the General Comment №25 on the UN Convention on the Rights of the Child (hereunder – the UNCRC), adopted by the

Committee on the Right of the Child on 2 March 2021, explicitly stating that children's rights under the Convention are to apply to the digital environment, the Irish Commission for the Protection of Personal Data has issued a comprehensive guidance on the processing of children's data "Children Front and Centre: Fundamentals for a Child-Oriented Approach to Data Processing" (abbreviated as "the Fundamentals"). The Fundamentals stipulate 14 child-specific data protection interpretative principles for organisations to reduce the data processing risks posed to children by the use of and getting access to online services: providing a minimum level of managing the security of personal data (a so-called "floor" of protection for all users), a "clear-cut" consent, which comes as the legal basis for processing through freely given, specific, informed and unambiguous statement, child-oriented transparency regarding children's audiences and prohibition of profiling (or automatic processing of personal data aimed at defining personal aspects of a natural person) of a child. [2]

The Irish Fundamentals consider the imbalance of power the user-child may possess in relation to online interaction and solve the problem by implying the obligation for controllers to ensure consent is "freely given." This formulation seems to suggest consent to be *understandable* for young users. Obviously, it is only through respecting this condition that it will be made possible to rely on consent as the legal basis for processing children's data.

In addition to the principal GDPR provisions, the specific Fundamentals also include such models of interaction as:

- "Zero interference relying on a child's best interests": allows organisations to rely on legitimate interests as a core legal basis for processing;
- "Know your customer" procedure focused on child-oriented transparency;
- Specific guidance around age verification and consent.

By implying the above-mentioned requirements, the Fundamentals aim at protecting the best interests of children and setting a default floor of high standardised protection for all data subjects including the minor user audience. [7]

Likewise, the Age-Appropriate Design Code (abbreviated as the Children's Code) concerning processing of personal data of children using commercial information society services, such as streaming services, online games, applications, news and education portals, came into force in Great Britain a few months ago (in December 2021). The Children's Code was designed to provide a risk-based approach to protecting children's personal data, keeping the balance between the free usage of benefits provided by online services to their young audience and 15 obligatory standards for companies engaged in minors' data collection work. In addition, there is an extraterritorial scope of the application: provisions of the Code apply whenever the company is a British legal entity or a foreign organisation specifically targeted at children including UK citizens. [4]

Today, as regulatory controls of minors' privacy are being actively implemented by European governments in the digital arena, U.S. legislation is setting its own standards to provide adequate protection of children's privacy interests. From the year 2000 onwards, the Children's Online Privacy Protection Act came into force on a federal level in the USA and has made a commendable development in reducing the risks to the rights and freedoms of children that may appear in the process of accessing the services through digital and online technologies. Notably, provisions of Children Online Protection Act (abbreviated as the COPPA) firstly established the principle of zero interference with the best interests of a child (zero-data process) including norms to abolish the processing operations consisting of profiling and targeted/ behavioural advertising activities related to the child's personal data. [3]

Let's consider and compare the legislative approaches in other countries. By "legislative approaches" we mean the range of legislative responses addressing the dynamics of

the data protection and privacy relations. Depending on various national legislations' frameworks and different personal data classification, the scope of regulation and penalties for data privacy infringement are different. For example, as for the Chinese privacy regulation, The Personal Information Protection Law of the People's Republic of China (shortened to PIPL), a federal data privacy law went into effect on 1 November 2021, establishing a set of rules on methods for the collection, use, processing, and transfer of personal data. The PIPL lays down key legal compliance initiatives on the part of Chinese legal entities and foreign organisations operating in China and enhances the existing data protection regime of handling of children's personal data laid down in 2019 by the Provisions on Cyber Protection of Personal Information of Children (abbreviated as the PCPPIC). Some specific requirements as defined prior to Article 29 of the PCPPIC relate to the collection, storage, use, transfer, and destruction of children's personal data within the PRC territory online. The provisions of PIPL, inter alia, include the obligation for data controllers to implement particular methods for protecting children's personal data that are automatically classified as "sensitive information". [8]

In respect of operators (people handling various privacy-related activities towards a child, like collecting or processing, the principle of "minimising authorization" is established by Articles 16 and 17 of the Regulation: each network operator shall establish strict access requirements for employees who use the personal data of children as part of their work responsibilities. [6]

Ukrainian legislation, for its part, introduced the draft Law "On Personal Data" of 6 July 2021, following the principles of proportionate data collection in the interests of the child.

We showed that countries follow the line of main international legal instruments on data protection, such as fundamental right and international standards of protection of privacy recognized by the United Nations and EU General Data Protection Regulation which provided impetus to global changes in this field.

Also an overview of Russian legislation (Federal Law of 27 July 2006 No. 152-FZ on Personal Data, Articles 23 and 24 of the Constitution of the Russian Federation of 12 December 1993; Federal Law of 27 July 2006 No. 149-FZ on Information, Information Technologies, and Protection of Information, Federal Law No. 149-FZ on Information, Information Technologies and Information Protection (2006) and Chapter 14 of the Labour Code of the Russian Federation (2001) with subsequent changes) showed the similar approach to the scope, principles of data collection and processing, obligations for data operators and based on the international instruments on privacy and data protection in certain aspects. However, few legal acts cut across the youth issue. Some of the requirements for the dissemination of information about a minor in the mass media are established by the Law of the Russian Federation "On Mass Media" No. 2124-I of 27.12.1991 and the Federal Law of the Russian Federation "On the Protection of Children from Information Harmful to their Health and Development" No. 436-FZ of 29.12.2010. Through the implementation of the minors' personal information regulation existing the Article 1.1. 64 of the Family Code of the Russian Federation and p. 3, Article 3, Article 9 of the Federal Law of the Russian Federation "On the Protection of Personal Data" №152-FZ of 27.07.2006 it can be stated that the right to consent to the use of personal information about a child is vested in his or her parents (or legal representatives).

A similar specification was also introduced in the Republic of Belarus with the enforcement of the "Personal Data Protection" act on 15 November 2021. The act itself was developed to control the personal data security of each individual citizen including children, by bringing some requirements for the procedure for obtaining consent in terms of processing of a child's personal data. A same-titled law was also issued in the Republic of Uzbekistan: Article 21 of the abovementioned act lays down the following obligation: "For minor subjects, consent to the processing of their personal data in writing, including in the form of an electronic document, is

given by parents (guardians, trustees), and in their absence — guardianship and guardianship authorities."

Taken together, at the moment the legislators of the Eurasian Economic Union (EAEU) countries and most other Eastern European states are gradually moving to special regulation of personal data in relation to children and do not seek to unify all data subjects, taking into account the peculiarities of their self-awareness and the degree of vulnerability of each, thus forming requirements for organisations, mostly in the gaming industry, using the personal data of minors.

It is presumed that strict obligations shall be implied for controllers for the sake of children's privacy. However, what are the key criteria for the maturity threshold in terms of special data safety procedures? Legislators emphasise the need to define the minimum age limit for data processing subjects.

In the European Union, the general rules for the age restriction on the processing of personal data of a minor are enshrined in Article 8(1) of the GDPR, establishing that "the processing of a child's personal data is legal only if the child is at least 16 years old." Thus, in a situation when a child under the age of 16 is unable to give consent personally, it is provided by "a person who has parental rights in relation to the child". Article 8 of the GDPR provides for the possibility of EU member states to independently lower the age limit with a common minimum threshold of 13 years, therefore the age of consent varies in each of the EU member states. The UK Children's Code defines a child as "a person under the age of 18" with reference to the definition introduced in Article 1 of the aforementioned UN Convention on the Rights of the Child. In Germany, Lithuania, Slovakia, Hungary, and the Netherlands the age in question reaches 16 years; in Austria – 14 years; and in France – 15 years.

Following the §312.2 COPPA USA provision, the term "child" can be understood as referring to an individual under the age of 13. [3]

In the Chinese PCPPIC, a person under the age of 14 is considered a minor and, thus, is subject to protection. So far, the Chinese authorities have begun to pay special attention to the problems of gambling addiction among young people. For that purpose, mandatory registration under real names was officially introduced in a number of popular games, on a par with the expanded age limit in 2019: for example, PCPPIC applies a ban on persons under the age of 18 for playing between 22:00 pm and 8:00 am. [1]

The legislation of the Russian Federation, the Federal Law No. 152-FZ of 27.07.2006 "On Personal Data", in particular, does not indicate the age limit for processing personal data. At the same time, part 1 of Article 64 of the Family Code identifies a person under the age of 18 with the term "minor", whose rights are protected by parents and legal representatives. [5]

As for Belarusian legislation, 16 years is considered old enough for the data subject to reach the "age of consent" as said in paragraph 9 of Article 5 of the Law of the Republic of Belarus "On Personal Data Protection".

Thus, a lack of unification international approaches for determining the minimum age threshold of subjects requires companies in the gaming industry to either add resources for tracking regulations in targeted jurisdictions or give access to some of its products to underage users.

In order to understand issues of organisations we evaluated requirements in different jurisdictions.

Organisations can independently determine the mechanisms for verifying the age and authentication of the data subject, provided that this mechanism shall not contradict any of the abovementioned requirements and principles. However, determining the optimal way to balance

children's rights and the commercial benefits can pose a lot of difficulties for optimising an online platform's processes.

A comprehensive list of requirements is found in the provisions of COPPA USA, specifically §312.5 (b), under which verification of a parent's consent shall be carried out in the following ways: by signing the consent & sending it via e-mail, or transactions with payment systems or through video/audio communication with company representatives.

The requirement to ensure transparent information and communication regarding the rights of the data subject as well as the regime for exercising said rights is prescribed in the general rule of Article 12 of the GDPR.

At this stage, a hardest moment comes for both controllers and data operators due to (1) increased control over minors' access to the service – and, consequently, the complication of the process of collecting the necessary information on the identity of the child/parent, and (2) the development of a tendency to minimise the amount of data being collected and limit the purpose of its collection. Today, there is no legally established detailed procedure for age verification or obtaining parental consent.

Furthermore, the legal basis for processing shall be taken into account. In countries regulated by Article 6(1) (f) of the GDPR, companies can use legitimate interest as a legal basis for processing children's data, provided they take particular caution to balance minor's rights.

A balanced approach between the legal basis for processing composes a complicated task for the controller and contains some peculiarities relating to national legislation. E.g., in Ireland the vital interests of the child may form the legal basis for processing. According to the Fundamentals, "the GDPR and data protection in general, should not be used as an excuse, blocker or obstacle to sharing information where doing so is necessary to protect the vital interests of a child or children."

This forms the obstacle for organisations to use legitimate interests as the legal basis for processing children's information, as it actively contradicts a zero-tolerance approach in this provision of the Fundamentals. It is explained by the Irish DPC guidelines, prescribing that "the child's interests or fundamental rights should always take precedence over the rights and interests of an organisation which is processing children's personal data for commercial purposes."

Therefore, in circumstances where the choice between the best interests of the child and a legitimate interest is required, the best interests of the child takes precedence.

In most national legislations, when defining a legal basis for data processing of a child, parental or legal guardian consent tends to be enough. Still, given the primary focus on a child's best interests, there are cases in which said interests may not be subject to consent. E.g., Brazilian law allows the exceptions to Article 14, Section 1 of the LDPR, requiring parental consent when processing children's data. As stipulated in Section 3 of the article in question, children's personal data may be collected without the consent when contacting the parents or a legal guardian is necessary, and as long as the data is used once and is not stored, or for their protection, and under no circumstances shall the data be passed on to third parties without consent as provided in §1 of this Article.

In the scenario described above obtaining consent may be impossible, for example, when there is physical separation between the child and the parents, that's why the child's best interest will be prioritised over parental consent. [9]

It should be noted that violating the requirements of personal data security entails corresponding responsibility both to the organisation that collects and stores data and to its partners.

Practice shows that in order to ensure compliance with GDPR requirements and national regulations, manufacturers of children's online platforms should take into account modern approaches to product monetization. Many gaming platforms regularly provide users with the opportunity to make purchases inside the system (or loot boxes, in other words).

Thus, any violation of the requirements regarding personal data entails strict liability in accordance with the GDPR – a fine of up to 20,000,000.00 euros or 4% of the company's annual global income – as well as in national NPAs. For instance, a breach of personal data protection requirements according to the legislation of the EAEU countries, such as Belarus, Russia and Kazakhstan, entails administrative or criminal liability.

The maximum administrative fine in the Republic of Belarus reaches up to 200 Belarusian roubles (Article 23.3 of the Code of the Republic of Belarus on Administrative Offences), up to 75 thousand Russian roubles – in the Russian Federation (Article 5.39 of the Code of the Russian Federation on Administrative Offences). The Code of the Republic of Kazakhstan on Administrative Offences, in turn, determines the amount of responsibility based on the growth indicators of an organisation – a fine of up to seven monthly calculation index is imposed for violations of personal data protection requirements by large businesses (Article 79 of the Code of the Republic of Kazakhstan on Administrative Offences).

Current research appears to support the need for cooperation between the state and business. A good example of the involvement of private organisations in ensuring an appropriate level of protection of personal data of minors can be seen in the application of the kidSAFE voluntary certification procedure. [10]

Designed independently from the GDPR, this certification effectively contributes to an assessment of the impact on the protection of personal data, thus, it doesn't constitute a substitute for the DPIA procedure in the EU (PIA in the USA). By passing the kidSAFE certification, the business can determine a particular risk, for which the working body – in this case, EDPB – will be required to establish a list of processing operations for the introduction of further changes.

Thus, the kidSAFE international certificate either enables to define the credible rating of a particular organisation or show its feasible reputational losses, since the legal force of such a certificate doesn't make sense without independent verification by the controller, the DPO, and, after all – by the supervisory authority and the European Council for Personal Data Protection.

3. Conclusion

Based on the foregoing, our results show that with respect to the EAEU countries' legislation unlike EU and USA legislation, lack of special regulation for the processing of minors' data is a rising issue.

Among the participants of the EAEU (Russia, Armenia, Belarus, Kazakhstan, and Kyrgyzstan) Russia was taken as the first country adopted Data Protection Law, the Republic of Belarus was taken as an example of reflection to GDPR's main principles and rules. It is important to notice that other EAEU countries are not directly apply EU General Data Protection Regulation on their territory but follow the common mainstream.

Taking into account the high risks and peculiarities of working with information regarding children's personal data, their role in the gaming industry market, which is growing its volume, it is possible to point out the following legislative requirements for online gaming services' *legal purity*:

- to define the age limit for minor data subjects, information about which will belong to the category of "sensitive data";

- to highlight the requirements for granting minors access to gaming services: confirmation of consent by parents; the procedure for identification and age verification;

- to implement the principles of "data minimization" and "goal restriction" for minors through greater anonymization of the data subject (for example, by introducing a ban on targeted advertising or restrictions for monetization of games aimed at a children);

- to develop and provide clear recommendations for data controllers on the processing of minors' data, on the provision by data controllers of clear, complete and understandable privacy policies for minors;

- to promote and use certification procedures for online platforms and services aimed at a children's audience, including allowing the usage of international certificates and giving them proper legal force, for example, the use of kidSAFE certification.

Acknowledgements

This research did not receive any specific grant from funding agencies in the public commercial, or not-for-profit sectors.

The authors declare no competing interests.

References

[1] DFT. China has officially introduced a facial recognition system to help track minors' playing at night. Retrieved 26 September 2021, from https://dtf.ru/life/788877-v-kitae-oficialno-vnedrili-sistemu-raspoznavaniya-lic-ona-pomozhet-otslezhivat-nesovershennoletnih-igrayushchih-po-nocham.

[2] DPC Ireland. The "Children's Fundamentals" – A guide to protecting children's personal data (2022). Retrieved 26 September 2021, from https://www.google.com/url?q=https://www.dataprotection.ie/index.php/en/dpc-guidance/blogs/the-children-fundamentals&sa=D&source=editors&ust=1630927401119000&usg=AOvVaw3c30xBtad35kvpK9MytNzF.

[3] Federal Trade Commission USA. Children's Online Privacy Protection Rule ("COPPA"). Retrieved 26 September 2021, from https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule.

[4] How to protect a child's personal data and who takes responsibility. Retrieved September 26, 2021, from https://nskdeti.nso.ru/page/1122.

[5] Information Commissioner's Office UK. Age-Appropriate Design Code, the Children's Code. Retrieved 26 September 2021, from https://ico.org.uk/for-organisations/age-appropriate-design/additional-resources/introduction-to-the-childrens-code/.

[6] LOC China. Regulation on Online Protection of Children's Personal Information Issued. Retrieved 26 September 2021, from https://www.loc.gov/item/global-legal-monitor/2019-10-28/china-regulation-on-online-protection-of-childrens-personal-information-issued/.

[7] Marie Daly. Irish DPC Publishes Guidance On Processing Children's Personal Data (2022). Retrieved 6 March 2022, from https://www.insideprivacy.com/childrens-privacy/dpc-publishes-guidance-on-processing-childrens-personal-data/.

[8] Morganlewis. PERSONAL INFORMATION PROTECTION LAW: CHINA'S GDPR IS COMING. Retrieved 26 September 2021, from https://www.morganlewis.com/pubs/2021/08/personal-information-protection-law-chinas-gdpr-is-coming.

[9] Processing children's personal data under Brazil's LGPD (2021). Retrieved 6 March 2022, from https://iapp.org/news/a/can-mandatory-consent-be-optional-processing-childrens-personal-data-under-brazils-lgpd/.

[10] Samet Privacy. kidSAFE® Seal Program. Retrieved 26 September 2021, from https://www.kidsafeseal.com/aboutourprogram.html.


C O A S