ZESZYT PRAWNICZY UAM
NR 14/2024
https://doi.org/10.14746/zpuam.2024.14.4

ISSN (ONLINE) 2956-2767
ISSN (PRINT) 2720-2526

PAULINA KLISOWSKA

Adam Mickiewicz University, Poznań, Poland
https://orcid.org/0009-0000-1866-8226
paukli3@st.amu.edu.pl

Parental Confirmation of a Child's Consent to Data Processing

Abstract: This article attempts to define the conditions for consenting to the processing of children's personal data under the GDPR. The article focuses on analysing the data protection law, regarding to the most important problem, that at present, consent to data processing involves at most a few clicks or nudges, making it difficult to speak of any real control of data controllers over whether consent to the processing of a child's personal data has been lawfully given or confirmed by an authorized person. It's not hard to see that the young age of users, along with limited awareness of data protection and the risks associated with its use, makes this topic extremely relevant and worth addressing.

Keywords: child's personal data, parental consent, GDPR, information society services

Introduction

The digital revolution has changed and is still changing the way people live. Young users' online activity and the risk to their privacy arising from less awareness of their rights are topics increasingly addressed and analysed by researchers.

The number of hours children and young people spend using social media and the internet continues to increase year on year. According to a study commissioned in 2021 by the Polish Ombudsman for Children, the amount of time spent online increases with age of the children. Only 12% of 2nd-grade pupils (8 years) claim that they do not use the Internet after school, while 6th-grade primary school pupils (12 years) and secondary school students say the same in only 2% and 1% of cases, respectively.[1] Therefore, it comes as no surprise that this generation is called Generation Z, or the Internet Generation (born 1995–2012).[2] The analysis in the present study also shows that 15% of 2nd-grade pupils feel bad when their access to social media is limited.[3] In relation to older groups of respondents, the results were similar—14% of the 6th-grade pupils and 15% of the secondary school students say the same.[4]

[1] Rzecznik Praw Dziecka, *Ogólnopolskie badanie jakości życia dzieci i młodzieży w Polsce. Obszar 5: Korzystanie z mediów społecznościowych i internetu*, Warszawa 2021 <https://brpd.gov.pl/wp-content/uploads/2022/01/Raport-RPD-korzystanie-z-mediów-społecznościowych-i-internetu-PDF.pdf> [accessed: 21.11.2023], p. 23.

[2] Statistics Canada, *Generations in Canada* <https://www12.statcan.gc.ca/census-recensement/2011/as-sa/98-311-x/98-311-x2011003_2-eng.cfm> [accessed: 21.11.2022].

[3] Rzecznik Praw Dziecka, op. cit., p. 21.

[4] Ibidem.

Thus, it is not difficult to see that the young age of the social media users, along with their low awareness of data and privacy protection, in general, pose a threat to their privacy and personal lives, as well as making them an easy target for fraudsters, who might find it tempting to try and phish their personal data.

In the General Data Protection Regulation,[5] the EU legislator took the above-mentioned changes into consideration and obliged data controllers to provide for special protection of children's data—article 8(2) GDPR. The GDPR stipulates that such special protection is necessary in cases where the child is below the age of 16 years—article 8(1) GDPR. However, it is important to consider whether the specific procedure for consent to the processing of children's personal data in relation to information society services arising from Article 8 of the GDPR can actually protect them properly.

This article therefore aims to set out the conditions for giving consent to the processing of children's personal data in accordance with the GDPR, determining whether they can be practically implemented by controllers. In order to introduce readers to the topic, I will first explain the fundamental concepts of the data protection law. I will then present the legal provisions for the processing of the personal data of children including the issue of parental or legal guardian consent to such processing, and the obligations put on data controllers by Article 8 of the GDPR.

1. Processing of Personal Data under the General Data Protection Regulation

The protection of personal data should be considered a fundamental right of every individual, regardless of his or her age, and its protection derives from acts of European law. A person's right to privacy is guaranteed by Article 16 of the Treaty on the Functioning of the European Union[6] and Article 8 of the Charter of Fundamental Rights.[7]

These provisions do not shape any specific obligations towards the authorities responsible for data management, nor are they only a basis for defining them in the secondary law of the European Union.

---

[5] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC OJ L119/1, hereinafter: GDPR.

[6] Consolidated version of the Treaty on the Functioning of the European Union [2012] OJ C 326, 26.10.2012, pp. 47–390, hereinafter: TFEU.

[7] Charter of Fundamental Right of the European Union [2000] OJ C 326, 26.10.2012, pp. 391–407, hereinafter: CFR.

Currently, the main piece of secondary legislation on the protection of personal data in the European Union is the General Data Protection Regulation.[8] This regulation shapes the image of personal data protection within the European Union and ensures a sufficiently high level of protection. The abovementioned regulation entered into force on 25 May 2016 and became fully applicable on 25 May 2018, removing Directive 95/46/EC from the legal order, which, until then, was the only legal basis for the protection of personal data in Europe. By creating a new legal act, the EU regulator went a step further, because although the regulation partly coincides with the previous regulation—especially in the area of data processing itself—it nevertheless clarifies specific rights and obligations related to the protection of individual categories of personal data, while introducing new, detailed provisions on the very functioning of the data protection system at the same time. The EU legislator also decided to change the form of legislation for the protection of personal data in order to unify this law more fully and effectively throughout the European Union and ensure a high level of protection in all Member States. As it is becoming increasingly difficult to define the 'limits' of data processing itself, the introduction of a uniform data protection regime at European Union level seems not only appropriate but also necessary.

The changes in the field of data protection introduced by the GDPR significantly affect the handling of personal information in all areas of legal transactions, as there is no doubt that the processing of personal data touches almost every area of life and affects every person regardless of age.

It is important that the EU legislator has introduced new categories of data in the GDPR, which have been granted special legal protection. One category of such data is the data of children, which is linked with the main concern of this article because, as was said before, lower awareness of the risks and consequences of the processing of personal data and less knowledge of their rights concerning them makes them an easy target for phishers.

The conditions for the processing of personal data of minors in the framework of information society services are regulated in Article 8 of the GDPR. However, it is worth beginning with the definition of the term "data processing" itself, behind which, with technological progress, more and more operations hide.

The Regulation defines the "processing" of data as an operation or set of operations performed on personal data or sets of personal data, whether or not by automated means—article 4(2). In addition, it lists examples of operations which are considered "processing" of data, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclo-

[8] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data OJ L 281/31, 23.08.1996, pp. 18–24.

sure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction (GDPR).

The enumeration of examples of activities constituting the term "processing" of personal data reflects the main assumption of the EU legislator that it is not possible to determine *a priori* what activities do or may fall within the scope of the said term.[9] Constructing the definition of the term "processing" in such a way allows it to cover all activities carried out on personal data.[10]

With regard to the subject matter of this article, namely the special conditions to a child's consent in relation to information society services, it seems that the Court recognises that the term "processing" includes activities such as: the posting of personal data on a website,[11] the sending of text messages containing personal data, the interception, transmission, manipulation, recording, storage or transfer of audio and graphic data,[12] the transmission of the name and address of a subscriber or internet user,[13] the video recording of persons,[14] the transfer of personal data from an EU Member State to a third country,[15] the act of publishing a video which contains personal data on a video website where users can upload, view and share videos,[16] and the collection and disclosure by transmission of personal data of website visitors through a third party plug-in.[17] The 'processing' of data will therefore not only mean the activities of search engines, but also the publication of content containing personal data on social networks such as Facebook, Twitter, and services that allow for the publication of the image of individuals on video, i.e., TikTok, YouTube, Instagram.

The very use of "operations performed on personal data" in the definition of the term "processing of personal data" should be considered a specific definition of these specific operations. From the point of view of the data protection regime itself, the definition of these operations is of utmost importance, as this action links the entity obliged to comply with the GDPR with personal data, imposing on it an

[9] P. Litwiński, *Komentarz do art. 8 RODO*, [in:] P. Litwiński (ed.) *Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz*, Legalis/el. 2021.

[10] C. Kuner, *Commentary on article 4 pkt 2*, [in:] C. Kuner et al. (eds.), *The EU General Data Protection Regulation: A Commentary*, Oxford 2021, p. 119.

[11] Case C-101/01, *Bodil Lindqvist* [2003] ECR I-12971, ECLI:EU:C:2003:596, Legalis no. 67277, para 25.

[12] Case C-73/07, *Tietosuojabaltuutettu v. SatakunnanMarkkinapörssi Oy and Satamedia*, ECLI:EU:C:2008:727, Legalis no. 114052, paras 35–37.

[13] Case C-461/10, *Bonnier Audio AB and Others v. Perfect Communication Sweden AB*, ECLI:EU:C:2012:219, Legalis no. 458009, para 52.

[14] Case C-212/13, *FrantišekRyneš v. Úřad pro ochranuosobníchúdajů*, ECLI:EU:C:2014:2428, Legalis no. 1162714, para 25.

[15] Case C-362/14, *Maximillian Schrems v. Data Protection Commissioner*, ECLI:EU:C:2015:650, Legalis no. 1385645, para 45.

[16] Case C-345/17, *Sergejs Buivids*, ECLI:EU:C:2019:122, Legalis no. 1878372, para 39.

[17] Case C-40/17, *Fashion ID GmbH & Co. KG v. Verbraucherzentrale NRW eV*, ECLI:EU:C:2019:629, Legalis no. 2194759, para 76.

obligation to protect personal data and also obliging it, pursuant to Article 35 of the GDPR, to complete an assessment of the impact of the operations performed on the system of personal data protection in the obliged entity.

2. Consent According to the Article 29 Working Party

Returning, however, to the problem of processing the personal data of children and the consent for such an operation, as mentioned above, Article 8 of the GDPR describes the conditions for consent to the processing of personal data by a child in a specific case of information society services. The level of protection of children's personal data is, and should be, higher due to the fact already emphasised of it being possible that they are less aware of the risks, consequences, and rights they have in relation to the processing of their personal data. This special type of protection, listed in recital 38 of the GDPR, primarily concerns the use of children's personal data for marketing purposes, the creation of personal profiles, user profiles, and the provision of services aimed directly at children. However, the use of the term "in particular" clearly indicates that the protection itself would not be limited to these marketing or profiling purposes, but should also cover the collection of children's personal data in the broadest sense.

It should be noted that Directive 95/46 does not specifically identify children's personal data as a separate category of data and thus does not provide special protection for them, which is why the problem of their protection was brought up during the work of the Article 29 Working Party. In particular, the problem of consent itself for the processing of children's data was raised, as it was and still is not clear who should give it and when. The work of the Article 29 Working Party focused on the obligations of parents and data controllers arising from such processing.[18] As the provisions of Directive 95/46/EC did not lay down rules concerning the processing of personal data of minors, the Article 29 Working Party included guidance on the application of the general data protection rules to this specific group of natural persons—children—in one of its opinions.[19] The document points out that, as far as possible, the decision to process personal data should be taken independently by the child or together with his or her legal representative, but considering, first and foremost, the child's welfare and wishes. This should, of course, also take into account the degree of maturity and awareness of the child's rights and obligations in relation to the processing of personal data.

[18] Article 29 Working Party is an independent European working party which until 25 May 2018 (entry into force of the GDPR) dealt with privacy and data protection issues <https://edpb.europa.eu/about-edpb/more-about-edpb/article-29-working-party_pl> [accessed: 22.09.2023].

[19] Article 29 Working Party Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools) [2009] WP 160.

These guidelines, as the name suggests, are an element of soft law and do not contain specific information on what age determines the different phases of a child's action and interaction with his or her legal representative in giving consent. It is therefore difficult to speak about the practicality of this opinion.[20] However, it is worth noting that this opinion contains some important rights and interpretative guidelines on the protection of children's personal data, which is why it had to be mentioned.

One of the aforementioned rights is the right to give a child whose data is processed because of parental consent an opportunity to withdraw consent upon reaching maturity.[21] In the framework of this right, the Article 29 Working Party stressed that it is essential that the controller obtains an explicit consent of the child from the child him- or herself once he or she has reached maturity in order to be able to continue processing his or her data lawfully.[22] The opinion also noted the need to impose an obligation on the controller to disclose information not only to the child's legal representative but also to the child him- or herself.[23]

The opinion highlights the key principles and values that should guide both the controllers and legal guardians of minors when deciding on the processing of their data. The Article 29 Working Party singled out the best interests of the child as the main legal principle.[24] In addition, the opinion listed the protection and care necessary for the well-being of children, their right to privacy, the right to legal representation in order to fully exercise their rights, and the right to participate in decisions that affect them.[25] The listing and highlighting of these specific rights by the Article 29 Working Party is important insofar as it provides some basis for interpreting the existing legislation, so it would be unreliable to omit the opinion from discussing these provisions.

3. Consent According to the General Data Protection Regulation

With above considerations in mind, the GDPR, in comparison with the previous regulation, provides special and additional protection for the processing of not only special categories of data, but also indicates particular groups of individuals whose data should be especially protected, setting specific requirements for administrators and processors. Such a group are in fact children.

[20] P. Litwiński, op. cit.

[21] Article 29 Working Party Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools) [2009] WP 160.

[22] Ibidem.

[23] Ibidem.

[24] Ibidem.

[25] Ibidem.

Article 8 of the GDPR is the first legally binding (the opinion of the Article 29 Working Party was only indicative) provision touching on the subject of data protection of children, which introduces additional obligations to ensure a particularly high level of protection of children's data. This provision stipulates that if the grounds for the processing of personal data, according to Article 6 of the GDPR, are consent, in the case of information society services offered directly to a child, it is lawful to process the data of a person who has reached the age of 16. But if the child is under the age of 16, the processing of his or her data is lawful only if consent has been given or approved by the person exercising parental authority or custody over the child, and only in the scope of consent given. The provision in question, however, only applies if two conditions set out in Article 8 are met—the data processing is related to an offer of information society services addressed to the child, and it is based on the premise of consent.

The "information society services" referred to in this particular provision of the regulation are, with respect to Article 1(1)(b) of directive (EU) 2015/1535,[26] all services provided for remuneration, at a distance, by electronic means and at the individual request of the recipient of such services, and therefore, in order to speak of an information society service, it must be examined whether the service in question meets all of these conditions. It is important to note that the term being developed refers to services provided without the simultaneous presence of the parties, which are sent and received at their destination by means of electronic equipment and which are entirely transmitted, conveyed, and received by wire, by radio, by optical means or by other electromagnetic means at the individual request.[27] Due to the development of technology, more and more categories are included in the information society services. According to the ECJ, the term "information society services" covers services for the sale of goods and services that make it possible to complete an electronic transaction online.[28] These include, but are not limited to, online financial services (e.g., e-banking), and sale of other services, e.g., tourism, online shops (sale of clothes, books, music, cosmetics, sale of mobile applications, games, etc.).

The provision of Article 8 of the GDPR is therefore applicable to the information society services in question, thereby leaving out of scope all those situations where the collection of consents takes place out of context of the provision of information society services. This shows the very specific and narrow scope of this provision. Moreover, these services must be conditionally offered directly to the child. The

[26] Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (codification) [2015] OJ L 241, 17.09.2015, pp. 1–15.

[27] Ibidem.

[28] Case C-108/09, *Ker-Optika bt v. ANTSZ Dél-dunántúli Regionális Intézete*, ECLI:EU:C:2010:725, Legalis no. 266050, para 25.

literature highlights that the interpretation of this element can go in two different directions.[29]

First, only content that is offered directly and exclusively to children can be considered as services offered directly to a child as per Article 8 of the GDPR; according to this interpretation, the provision covers only services intended exclusively for persons under 16 years of age. This could be sites with computer games, books for children and young people, fairy tales or films for young people.[30] The main problem with this interpretation is that social networking sites that target all age groups, not just minors under 16, are excluded from the scope of the provision. The data controller must therefore be aware of the possible differences between the regulations of different Member States, taking into account the target audience of its services. In addition, from the perspective of national law, it should be noted that the controller who provides cross-border services cannot always rely on the compliance of its actions with the law of the Member State in which it has its organizational unit.[31] Member States are allowed to choose as a point of reference in their national law either the place of establishment of the service provider or the place of residence of the person whose data is to be processed. The condition is that this choice should be made with regard to the welfare of the child.

In the second case, an interpretation is made using the criterion of accessibility.[32] According to this interpretation, a service addressed to children will also be considered as a service which, due to its general accessibility, can be used by children. Here, in turn, a problem arises in relation to the obligations of controllers. As this interpretation of the provision recognizes that the specific protection of children's data under Article 8 of the GDPR applies to all publicly accessible services on the internet, and therefore, regardless of whether the content they offer is dedicated directly to children, the controllers of these services are obliged to comply with the obligations under this provision.

In order to facilitate the interpretation of this particular provision, reference should be made to the guidelines on consent drawn up by the European Data Protection Board (EDPB), which state that if a service provider informs potential users that the service it provides is directed at adults, and if nothing contradicts this assumption (e.g. the content of the website or marketing plans), then the provisions of Article 8 of the Regulation do not apply.[33] The European Data Protection Board (EDPB) itself upholds the principles of the GDPR. The EDPB is a body of the Euro-

[29] P. Litwiński, op. cit.

[30] Ibidem.

[31] Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1 adopted on 4 May 2020, pt 130 <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_pl.pdf> [accessed: 5.05.2024].

[32] P. Litwiński, op. cit.

[33] Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1 adopted on 4 May 2020, pt 130, op. cit.

pean Union which was established by Article 68 of the GDPR. It is an independently operating body that works towards the consistent application of data protection principles across the European Union and promotes cooperation between EU data protection authorities. The duties of the EDRB include the following: monitoring the correct application of the GDPR, advising the European Commission (EC) in the field of data protection law, issuing guidelines, recommendations, and best practices, reviewing the practical application thereof, examining of questions covering the application of the GDPR. Moreover, the European Data Protection Board cooperates with international organisations and supervisory authorities of non-EU countries to ensure a more effective enforcement of the right to data protection, exchanges practices and organises joint training programs. The European Data Protection Board was created to replace the Working Party on the Protection of Individuals with regard to the Processing of Personal Data (the Article 29 Working Party), which was established by Article 29 of Directive 95/46/EC, and, until 25 May 2018 (namely until the entry into force of the General Data Protection Regulation), dealt with privacy and data protection issues.

Article 8 of the GDPR establishes an age limit for the ability to consent to the processing of personal data in the case of information society services offered specifically to a child. According to the aforementioned provision, this limit was set by the EU legislator at 16 years. In essence, the GDPR leaves it up to the Member States to decide whether to lower the age limit from 16 to a lower one, however, not lower than 13. The Republic of Poland has not decided to lower the age limit; hence, the 16-year limit remains in force.

According to Article 8 of the GDPR, if the child is under 16 years of age, the processing of his or her data is only lawful if consent has been given by the person who has parental authority or custody of the child. In this case, consent is considered legally binding in two cases: when it has been given by the guardian instead of the child, and when the consent given by the child has been confirmed by the child's parent or legal guardian. The EU legislator has therefore imposed an obligation on the controller to ascertain whether the actual consent has been lawfully given using the technology available to him and reasonable efforts.

The GDPR does not specifically identify cases where the child could make the decision himself or herself and the guardian only approves it, so it is necessary to refer to the theses formulated by the Article 29 Working Party discussed above regarding the child's well-being and will, depending on the child's maturity and awareness.

This provision of the GDPR therefore implies an additional obligation on the part of the data controller, which in order to obtain consent from the child, must explain the purpose and the way they intend to process the child's data, using language the child can understand.

Furthermore, age verification itself should not expose the data to excessive processing and the mechanism chosen by the data controller to verify the age of

the person whose data will be processed should also include an assessment of the risks associated with the processing itself. As an example of the fulfilment of the requirement to confirm the age of the person whose data will be processed, the EDPB itself suggests, in low-risk situations, requiring a new subscriber of the service to disclose his or her year of birth, or filling out a form stating that he or she is or is not a minor.[34]

Referring, on the other hand, to persons under the age of 16, the GDPR by itself also does not provide specific, practical ways to obtain a parent/guardian's consent or confirmation of the consent given by the child. The EDPB recommends again that a proportionate approach should be adopted, which is to seek a limited amount of information, such as parent's or guardian's contact information.[35] In the same way, the administrator can determine whether the person who gave or confirmed the consent is an authorised person.

The rationality of the verification measures taken may depend on the risks involved in the data processing and the technology available to the controller. In a low-risk situation, confirmation via email may be sufficient for verification purposes; in a high-risk situation, other evidence may be appropriate.[36]

By taking reasonable measures already at the stage of confirming consent, the data controller is able, in the event of any complaints, to prove that he or she has taken reasonable measures and made appropriate efforts to ensure that his or her data processing is carried out lawfully.

Summary

It is important that a problem as crucial as the protection of personal data of children has been noticed and a solution has been implemented. However, what this article proves is that many serious problems regarding data protection have been left unsolved and unanswered by the GDPR.

What can be seen from the considerations in this article is that the GDPR lays down a very comprehensive foundation for the protection of personal data of children. However, what the GDPR requires of data controllers in terms of ascertaining that a parent or a legal guardian of a child under the age of 16 has in fact given or confirmed the consent for the processing of the child's data can hardly be verified. However, it is important to note that the duties of data controllers outlined above are duties of diligence. It is the controller who should ensure that the measures it takes, in order to verify that consent to the processing of a child's personal data has been lawfully given, are proportionate to the purposes and nature of the processing

[34] Ibidem.
[35] Ibidem.
[36] Ibidem.

activity and the risks involved in it. This follows the fact that it is the controller's responsibility to determine what measures should be taken in a particular case, with the aim of avoiding solutions that require excessive collection of personal data.

Given that nowadays giving consent for the processing of data requires at most a couple of clicks, it is difficult to speak of any actual control by data controllers over whether the consent for the processing of personal data of a child had been lawfully given or confirmed by the child's parent or legal guardian. Therefore, the solutions indicated by EDPB, although helpful, will unfortunately not always be sufficient to determine whether the consent to process the child's data was given in accordance with the existing regulations.

BIBLIOGRAPHY

Kelleher, D., Murray, K. (2021). *EU Data Protection Law*. London.

Krzysztofek, M. (2016). *Ochrona danych osobowych w Unii Europejskiej*. Warszawa.

Kuner, C. (2021). *Commentary on article 25*, [in:] C. Kuner et al. (eds.), *The EU General Data Protection Regulation: A Commentary*. Oxford.

Litwiński, P. (2021). *Komentarz do art. 8 RODO*, [in:] P. Litwiński (ed.), *Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz*. Legalis/el.

Sakowska-Baryła, M. (2018). *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*. Warszawa.

Tosoni, L., Bygrave, L.A. (2020). *The EU General Data Protection Regulation: A Commentary*. Oxford.