ISSN 2029-1701
ISSN 2335-2035 (Online)

Research Journal
PUBLIC SECURITY AND PUBLIC ORDER
2022 (30)

FEATURES OF THE LEGAL REGULATION ENSURING THE RIGHT OF MINORS TO PRIVATE LIFE AND THE PROTECTION OF PERSONAL DATA

Eglė ŠTAREIKĖ
Mykolas Romeris University
Maironio st. 27, LT 44211 Kaunas
Tel.:+370 656 76033, E-mail: egle.stareike@mruni.eu,
ORCID ID:0000-0001-7992-991X

DOI: 10.13165/PSPO-22-29-11

Abstract. *The quality protection of minor's right to privacy cannot be achieved without sufficient protection of personal data. The General Data Protection Regulation provides specific protection rules for the processing of minor's 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. Minors merit specific protection, any information and communication when it comes to their privacy and data protection.*

This scientific article aim is to investigate the legal regulation for the protection of minors's personal data and to show the connection of this legal regulation with the individual's fundamental right to privacy and identify the problems of this legal regulation.

In order to achieve these goals, there will be discussed the main legal aspects of children's data protection, such as consent, age requirements and other aspects. This scientific article analyzes not only the legal regulation of the protection of children's personal data but also the connection with the right to privacy.

Keywords: *right to privacy, minor's protection of personal data, GDPR.*

Introduction

Development of the information society, evolution of new technologies, processes of globalization, growth of the use of digital technologies due to the influence of the COVID-19 pandemic raise the debate about the impact of present and future technologies on human rights, i.e., how these processes can ensure and protect the human right to privacy and the protection of personal data. The mentioned processes have particularly highlighted the importance of the right of minors to data protection and privacy, and at the same time have led to a new look at the problems arising from the improper processing of personal data.

The personal data protection system has been developed to protect not only personal data, but also person's right to private life. Importantly, the violation of the right to the protection of personal data also violates the privacy of the person (*Štareikė, Kausteklytė-Tunkevičienė, 2021*).

On May 25, 2018, a new legal regulation, the General Data Protection Regulation (GDPR) (*GDPR, 2018*), came into force, which took a fresh look at the problems arising from the improper processing of personal data (*Štareikė, Kausteklytė-Tunkevičienė, 2018*). It was the GDPR and its legal regulation that was the first in the European Union to regulate the processing of personal data of minors under the age of 16, classifying personal data of minors as particularly sensitive data requiring greater protection. The GDPR actually returned control of personal data from organizations to the natural person, transferring responsibility to them. Organizations must be able to explain to every natural person who asks them: What information about the person does the organization has? For what purpose it processes personal data? Where and how is the processed personal data used? (*SolPriPa Project Guidelines, 2019*).

The quality protection of the minors right to privacy cannot be achieved without sufficient protection of personal data. The General Data Protection Regulation provides specific

protection rules for the processing of minor's 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. Minors merit specific protection, any information and communication when it comes to their privacy and data protection (*GDPR, 2018*). Minors want to maintain control over their personal data, as this is related to the sharing of the value of personal data. Personal data can be used to better serve individuals on the internet, for example, to target ads that are relevant to them and meet their needs (*SolPriPa Project Guidelines, 2019*).

In this context, this article analyses the relationship between the minor's right to privacy and protection of personal data, legal regulation, scope of these rights and values protected. The second part of the article analyses the requirements for the processing of personal data of minors and the main measures to ensure the right of minors to data protection and privacy in the digital space.

The relevance of this scientific article is related to ensuring the processing of personal data of minors and privacy requirements and identification of appropriate measures to prevent violations of these rights. The **purpose of this scientific article** is to analyse legal regulation of the processing of personal data of minors and identify the problems of this legal regulation. In order to achieve these goals, there will be discussed the main legal aspects of minor's data protection, such as consent, age requirements and other aspects. This scientific publication will analyse not only the legal regulation of the protection of minor's personal data but also the connection with the right to privacy.

The object of scientific article is processing of personal data of minors as a guarantee of the right to a private life.

The scientific article uses the following theoretical and empirical methods: the method of comparative analysis, logical – analytical and systematic analysis. The comparative analysis method was used to compare the content and legal regulation of the right to protection of personal data of minors and right to privacy, a logical – analytical method was used to analyse the requirements for the processing of personal data of minors and to identify the most common problems in this area. Logical-analytical and systematic analysis methods are used to reveal the relationship between legal acts and legal doctrine, different legal norms, summarize the scientific article, reveal the main problem, and formulate conclusions.

Legal regulation of the right of minors to protection of personal data and protection of private life

The right to privacy and protection of personal data is governed by both the European Union (further – EU) and the Council of Europe (further - CoE) legal regulation ensuring protection of fundamental human rights. The right to privacy and protection of personal data are closely related, sometimes even overlapping, but they are not identical rights (although they protect similar values - human dignity, the right to autonomy, secrecy of personal life, etc.) (*Štareikė, Kausteklytė-Tunkevičienė, 2021*). Privacy and data protection, although interrelated, are recognized worldwide as two separate rights. In Europe, they are seen as vital parts of sustainable democracy and privacy is recognised as a universal human right, but data protection – at least for the time being - is not. The right to privacy or private life is consolidated in *The Universal Declaration of human rights* (Article 12), *The European Convention on Human Rights* (Article 8) and *The European Charter of Fundamental Rights* (Article 7).

The concept of data protection arises from the right to privacy, and both are important for preserving and promoting fundamental values and rights. Data protection has precise objectives

to ensure fair processing (collection, use, storage) of personal data in both public and private sectors. (*European Data Protection Supervisor*).

The Council of Europe's legal framework for the right to privacy and data protection is consolidated in various documents. One of the most important legislations guaranteeing the rights to privacy and data protection is the Convention for the protection of human rights and fundamental freedoms (*ECHR*) of the year 1950. Article 8 of the ECHR establishes a person's right to private and family life esteem: (i) everyone has the right to respect for his private and family life, his home and his correspondence; (ii) there shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

The 108th Convention of the Council of Europe, which was submitted for signature back in 1981, long before the era of internet and electronic communications, is also worth noting. The 108th Convention of the Council of Europe is the first binding international instrument that protects individuals against abuse that may involve the collection and processing of personal data, establishes basic principles and safeguards, and grants rights to data subjects. The development of digital technologies has raised new challenges and highlighted problems in the field of personal data protection. Considering the imperfection of data protection regulation the Convention was updated in 2018 (*Council of Europe, 2018*). Given different responsibilities of supervisory authorities, the Convention now clearly requires institutions to pay great attention to the rights of children and other vulnerable persons in data protection when it comes to raising public awareness (*Milkaite, Lievens, 2018*). The updated Convention sets out the objective of protecting the right to private life through automated processing of personal data, respecting the rights and fundamental freedoms of each person in the territories of all parties, regulating international data transfers and, in particular, ensuring the right to private life of individuals.

The international agreements are also worth mentioning. *The United Nations' Convention on the Rights of the Child* of the year 1989 is an important agreement between countries that have promised to protect and safeguard the rights of the child. The Convention regulates that any person under the age of 18 is considered a child. It also regulates what are the rights of children and what are the duties of the governments of the countries. All rights governed by the Convention are related, all are equally important and cannot be taken away from children. Clause 16 of the Convention provides for the protection of privacy, i.e., that every child has the right to privacy. It is also established that the laws of the States Parties to the Convention shall protect the personal and family life of children, the inviolability of the apartment, the secrecy of correspondence or any unlawful encroachment on their honour and reputation. The child has the right to be protected from such interference or encroachment by the law. Clause 17 of the Convention regulates children's access to information, States Parties recognise the important role of mass media and ensure that the child has access to information and materials from various national and international sources, in particular such information and materials that contribute to the child's social, spiritual, and moral well-being and promote his or her physical and mental development. It is recognized that children have the right to receive information from the internet, radio, television, newspapers, books, and other sources. In the meantime, adults should make sure that the information they receive is not harmful. Governments should encourage the media to share information from various sources in languages that are understandable to all children (*The United Nations Convention on the Rights of the Child, 1989*).

The protection of personal data of minors is subject to the general legislation of the European Union: the Charter of fundamental rights of the European Union, the General Data Protection Regulation (*GDPR, 2018*).

Article 7 of the Charter of Fundamental Rights of the European Union distinguishes between a person's right to private and family life, that every person has the right to respect for his or her private and family life, the inviolability of housing and the secrecy of communication. Article 8 establishes the protection of personal data, where each person has the right to the protection of his or her personal data, and personal data must be properly processed and used only for specific purposes and only with the consent of the person concerned or on other legal grounds established by law. An independent body must monitor compliance with the rules on the protection of personal data (*Charter of Fundamental Rights of the European Union, 2000*).

Table1. Legal regulation of the child‘s right to privacy and data protection
Source: compiled by the author

CoE legal regulation	EU legal regulation	National regulation
The European Convention for the protection of human rights and fundamental freedoms (Article 8)	Charter of Fundamental Rights of the European Union (Articles 7 and 8)	The law on legal protection of personal data of the Republic of Lithuania (Article 6)
The Convention of the Council of Europe No. 108+	General Data Protection Regulation (Article 8)	The law on information society services of the Republic of Lithuania (Article 10)
	The resolution of the European Parliament, dated July 6, 2011, on a comprehensive approach to the protection of personal data in the European Union (2011/2025 (INI))*	The law on the protection of the rights of the child of the Republic of Lithuania (Article 10, part 1)
	Article 29 Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*	
	Article 29 Working Party opinion 2/2009 on the protection of personal data of minors *(Opinion 2/2009 on the protection of children's personal data)* *	
	Article 29 Working Party working document 1/2008 on the protection of personal data of minors *(1/2008 on the protection of children's personal data (general guidelines and the special case of schools))* *	
	**Documents are of a recommendatory nature, i.e., not legally binding*	

.

On May 25, 2018, in the Member States of the European Union there was introduced the GDPR, repealing the October 24, 1995 Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the freedom of such data, on which the processing of personal data in the EU member states

was based. The aim of the GDPR to ensure real protection of personal data, to protect the rights of individuals in the digital space and to strengthen the fight against crime is identified as an incentive to have a uniform and updated legislation on the protection of personal data in all member states of the European Union. The main objectives of the personal data protection reform were to strengthen the rights of data subjects, to establish the responsibilities of data processors and data sub-processors, and to ensure transparent and reliable regulation and processing of personal data (*Štareikė, Kausteklytė-Tunkevičienė, 2018*). According to R. N. Zaeem and K. S. Barber (2020): *„The EU GDPR is one of the most recent and powerful regulations passed to protect consumers' data. Not only does it give EU citizens more agency to control their own personal information with organizations inside and outside the EU, the GDPR has inspired sweeping new legislation in the US and continues to be the most widely referenced privacy regulation as new regulations are considered in the US and around the globe".*

Frequent breaches of personal data are related to minor's personal data due to insufficient protection through the use of smart technologies. So, the question naturally arises is the privacy of minors sufficiently guaranteed by the regulations on the protection of personal data? The rapid growth of technologies and the provision of services, where the business model is based on the collection and analysis of personal data (from social networks, marketing, analytical purposes) pose many problems. The protection of personal data is a fundamental right of the EU and privacy is understood more than a luxury but a necessity (Livingstone, 2018).

Thus, the main aspects of how the GDPR is committed to improving the protection of minor's privacy are discussed. The GDPR has established that information related to personal data and held by data controllers and processors (Livingstone, 2018):

- first, process them lawfully, securely and fairly, in a transparent manner and in a way that is comprehensible to data subjects;
- second, collect and process personal data and, if data controllers engage in profiling, only for specific, explicit, and legitimate purposes, subject to specific provisions on "sensitive" data (e.g., health data; data on racial or ethnic origin; religious beliefs; information on sexual orientation, etc.).
- third, facilitate the rights of individuals to access, rectify, erase and restore their personal data in certain circumstances
- fourth, meet a wide range of management requirements based on risk-based impact assessments.

Personal data of minors are classified as particularly sensitive data requiring greater protection by excluding minors from the general spectrum of the concept of entities (see Table 2)

The GDPR Recital 38 establishes that the specific protection of minors is applied in cases where information society services are provided, because minors need special protection of their personal data, because they may not be sufficiently aware of the risks, consequences or safeguards associated with the processing of personal data and their rights. Such special protection should in particular apply to the use of minor's personal data for marketing purposes, the creation of a virtual personality or user profile and the collection of personal data relating to minors through the services offered directly to the child. The consent of the holder of parental responsibility should not be required to provide prevention or counselling services directly to the child.

Table2. Types of personal data
Source: compiled by the author.

Personal data	Special categories of personal data	Personal data of minors
Any information about identified or identifiable natural person (name, surname, tel. no, bank card no., fingerprint, iris, face image, vehicle registration no., e-mail address and so on.)	- Racial or ethnic origin, political views, religious or philosophical beliefs, trade union membership; - Genetic data, biometric data (to specifically identify a natural person); - Health data, - Data on the sex life/sexual orientation of a natural person.	**Personal data of minors classified as particularly sensitive data requiring greater protection by excluding minors from the general spectrum of the concept of entities** (name, surname, personal code, address of residence, telephone number, e-mail address, nationality, date of birth, bank card number, education data (completed primary school, data on diplomas and certificates), data on health (health status, blood group, etc.), image data, biometric data, family member data (if associated with the data subject), interests, purchase and shopping history, internet pages visited by a person, randomly generated telephone number, location data (e.g., location data on mobile), Internet Protocol (IP) address, etc.

Thus, according to the EU law (*Art. 8 of GDPR*), if information society service providers handle data of children over 16 years of age, on the basis of consent, such data processing will be legal only if that consent has been given or the processing of the data has been authorised by the holder of parental responsibility and to the extent that such consent or permission has been given. The State Consumer Rights Protection Service defines information society services as various economic activities carried out when connected to an electronic communications network, in particular the sale of goods via the internet. Information society services are not only services for which contracts are concluded on the internet, but also include those services for which their recipients do not pay, such as services for the provision of information on the internet, means for retrieving, accessing information, services consisting in the transmission of information via communication networks, the provision of access to the communication network or the provision of information provided by the recipient of the service on the internet (*State Consumer Rights Protection Authority*). Member states may set a lower age in their national law, but not less than 13 years. In accordance with GDPR 58, minors must be given special protection, and information and notifications where data processing is child-oriented should be worded in clear and simple language that is easy for the child to understand.

The law on the protection of the rights of the child of the Republic of Lithuania (*Art. 10, part 1*) affirms that the child has the right to private personal and family life, privacy of communication, protection of personal data, secrecy of correspondence, honour and dignity, inviolability, and freedom of the person.

The European Parliament resolution, dated July 6, 2011, on a comprehensive approach to the protection of personal data in the European Union (2011/2025(INI)) notes that children must be particularly protected, as they may not fully understand the risks, consequences, safeguards, and rights associated with the processing of personal data, given the increasing

number of social networks on the internet and the disclosure of their personal data by young people. Attention is drawn to the need for particular protection of vulnerable persons, especially children, in particular by establishing a mandatory requirement for a high level of data protection and implementing appropriate specific data protection measures for such persons; stresses the importance of data protection legislation; recognises the need for particular protection of children and minors, given the increased use of the internet and digital content by children, and stresses that the ability to use media should be an important part of official education in order to teach children and minors to behave responsibly in the online environment. In order to achieve the intended objectives, special attention should be paid to the provisions on the collection and further processing of children's data, the implementation of the principle of limitation of goals in the field of children's data.

With regard to profiling, the Article 29 Working Party, a former advisory body that provided guidance on the implementation of the EU data protection law, which was replaced by the European Data Protection Board established after the entry into force of the GDPR, pointed out that despite the fact that the GDPR does not prohibit profiling of children at all, data controllers should generally refrain from profiling (behaviour) of minors for marketing purposes (Article 29 Data Protection Working Party, 2018). Automated decision-making, including profiling, with legal or similar significant effects should not apply to minors. Profiling children from an early age can lead to ads, services, products, and information being tailored and targeted to them, based on their online presence and past behaviour, offering the same services and goods, thus reducing new opportunities (Milkaitė, Lievens, 2018).

Following an overview of the main legislation and the legal regulation of the processing of personal data, the main measures to ensure the right of minors to data protection and privacy in the digital space are discussed below.

Key aspects to ensure the right of minors to data protection and privacy in the digital space

In 2019, „Spinter tyrimai“ research on the issues of personal data protection was conducted in Lithuania on behalf of the State Data Protection Inspectorate in order to find out the opinion and awareness of the population regarding the protection of personal data (*State Data Protection Inspectorate, 2019*). The study revealed that 73 percent of 18-25 years old Lithuanian residents know or believe that they know about the rights or duties established for them by law in the field of personal data protection. Young people identify online media (58%) and television (52%) as the most popular source of information on personal data protection, while other people (28%) and social networks have similar popularity for disseminating information on personal data protection (27%) (SolPriPa, 2019).

In the light of the above study, the online space presents a number of challenges related to the processing of personal data, especially when online services and social networks are used by minors. In practice, many questions arise regarding the processing of personal data of minors: what information should be provided to minors about the processing of their personal data? Is the consent of a minor required to process his or her personal data? What is the age limit from which the data controller and/or the processor can process personal data of minors?

As already mentioned, the protection of personal data is closely related to a person's right to privacy. Violation of personal data processing requirements also violates the right to privacy. Ensuring the right to privacy is vital for the development of the child. Key privacy-related media literacy skills are closely linked to various areas of child development. Children are still developing their own awareness of privacy, but even older minors have difficulty understanding the full complexity of internet data flows and some aspects of data commercialization. There is

a clear need for an adapted approach that takes into account the social maturity and development of minors and individual differences. Not all minors are equally able to browse the digital environment safely, taking advantage of the opportunities available, avoiding or reducing privacy risks. These problems raise pressing issues in media literacy research and education. It is undeniable that privacy concerns have intensified with the introduction of digital technologies and the emergence of internet access, as these technologies create large data sets with detailed documentation of personal information about internet users. Meanwhile, minors are more vulnerable than adults to online threats to privacy because they lack digital skills and do not realize the risk of privacy violation (*Livingstone, Stoilova Nandagiri, 2019*).

The first aspect, it is important to note that any information that can help identify a person is personal data. Information should be understood as audio, visual, genetic data, fingerprints and other data, which can be represented by letters, numbers, graphic, photographic image, sound (phone) and other forms. Thus, personal data is considered all information related to:

1) Information relating to a living person;
2) A person's identity can be established by directly personally identifiable data (e.g., by name and surname, personal code, etc.);
3) Determined indirectly, i.e., when the available data is insufficient to identify a specific person, however, the identity of the person can be established using other data, regardless of whether the organization has it (e.g., car license plate number, video data, telephone number, etc.) (*SolPriPa Project Guidelines, 2019; GDPR, 2018*).

The controller must actively provide certain essential mandatory information to the data subjects. Information about the name and address of the data controller, the legal basis and objectives of processing, the categories and recipients of data processed, as well as the means for the implementation of rights can be granted in any appropriate format (electronic website, through technological means for personal devices, etc.), provided to the data subject in a fair and efficient manner. The information provided should be easily accessible, readable, understandable, and adapted to the relevant data subjects, for example in a language understood by children. Any additional information that is necessary to ensure fair processing or that is useful for such a purpose, such as retention period, knowledge of the reasons for the processing or information about the data transfer to another contracting or non-contracting party (including information whether that particular non-contracting party provides an adequate level of protection or whether the data controller has taken measures to guarantee that level of data protection) cases must also be reported (*Handbook on European data protection law, 2018*).

As already mentioned, Article 8 of the GDPR provides that, where personal data are processed on the basis of the consent of the person and this relates to the direct offer of information society services to the minor, the processing of the minor's personal data is lawful only if the minor is at least 16 years old, but not less than 13 years old. The Law on legal protection of personal data of the Republic of Lithuania establishes that the processing of personal data of a minor is legal if the consent is given by a minor not younger than 14 years of age. It should be noted that if a minor is under 14 years old and uses electronic services (social networks, receives newsletters, sends computer games) to data controllers - various business representatives need to obtain the consent of one of the minor's parents or other legal representatives, since the provision of these services will use the minor's personal data.

Personal data, as with other data subjects, must also be processed in accordance with the principle of transparency (*Štareikė, 2021*). Consent must be given freely, based on information, specific and unambiguous. Consent must be a statement or a clear confirmatory act expressing consent to the processing of data, and the person has the right to withdraw his consent at any

time. It is the responsibility of controllers to keep a verifiable record of consent that can be verified (*Handbook on European data protection law, 2018*).

Although the GDPR does not impose requirements on the form or ways in which a person's consent is to be given, it does establish these terms of consent (*SolPriPa Project Guidelines, 2019*):

1) The controller must be able to prove that the minor or his legal representative has agreed to the processing of personal data;

2) It must be ensured that the minor understands to whom and for what he has given his consent, and therefore he must be properly informed of:

- the identity of the company collecting personal data (i.e., name, legal entity code, etc.),
- the purposes of the intended processing of personal data,
- type of data to be processed,
- possibility to withdraw consent,
- the fact that the data will only be used for automated decision-making, including profiling (if applicable),
- transfer of data to third parties, etc.

3) The consent request must be made in an understandable and easily accessible form, in clear and simple language, and should not contain unfair terms;

4) Silence, pre-ticked boxes, inaction should not be considered consent;

5) Consent is obtained by a written statement (including by electronic means) relating to other matters, must be clearly distinguished from other matters;

6) Consent must not be ambiguous;

7) Revoking consent must be as easy as giving it. The person must be informed of the right to withdraw his or her consent before giving his or her consent.

Obviously, the fact that more and more human activities are being converted into data means that privacy, and no longer publicity, now requires a thoughtful effort, so that it is much easier to preserve than to remove a record of what has been said or done. It is becoming the norm, not the exception, that the digital footprint of personal data becomes a means by which a person's choices are determined by others based on their views and also on the interests of the controller (*Livingstone, Stoilova, Nandagiri, 2019*). Thus, the increasing use of digital technologies also leads to increased requirements and responsibilities for data controllers in order to properly process personal data of minors and in order to avoid penalties for improper processing of personal data of minors. Business representatives (data controllers/processors) should first be able to correctly identify and verify the age of a minor seeking electronic services. Business representatives should take proportionate measures to the nature and risks of data processing activities, to verify that the minor is of the age to give consent in the digital space, as an example, to ask questions that the minor would not be able to answer by his maturity, or not to provide services until the minor provides the e-mail address of one of his parents or legal representative.

Children under the age of digital consent must have the consent of the holder of parental responsibility on their behalf. Member states have the right to reduce this age to 13 years in one of the rare cases of derogation allowed by the GDPR. This means that in practice, when a child gives consent, he should confirm which country he is in, since different states may have different age restrictions (*Data Global Hub*). Thus, if the user is younger than required, the data controller will have to require not only parental permission for the minor to access the services in the digital space, but also to make sure that the person giving that consent is the holder of parental responsibility. In all cases, in order to verify the age of the minor, the principle of data minimisation should be respected, where personal data should only be processed using

appropriate means if the purpose of the processing of personal data cannot reasonably be achieved by other means (*Štareikė, 2021*). Where the risk is not high, data collection may be limited to the minor filling out an appropriate form on the internet – indicating his date of birth. Data protection impact assessment (DPIA) can help decide what steps need to be taken to verify a child's age, his/her state of residence, or the right of legal representatives to express their consent on behalf of the child. Under the current legislation, it is necessary to carry out DPIA when children are directly offered information society services (*State Data Protection Inspectorate, 2019; GDPR, 2018*).

However, according to S. Livingstone, M. Stoilova and R. Nandagiri (2019) ensuring minor's privacy in a digital environment is particularly challenging for three main reasons.

First, minors are often pioneers in exploring and experimenting with new digital devices, services, and content. Minors face risks that many adults do not even realize or are unable to predict risks, while developing risk reduction strategies. Although minors have always been experimental, today these actions are especially significant, since minors now operate on digital platforms that both record everything and are often owned by data controllers. The increasing monitoring and accumulation of data, the occasional and inappropriate use or leakage of personal data of minors, and therefore privacy, are a major concern in public and political circles.

Secondly, minors are less aware than many adults of the current and future risks posed to their well-being by the use of the digital environment. Most studies have focused on underage adolescents, but it is increasingly common for the youngest children to constantly use the internet (*Chaudron et. al., 2018; S. Livingstone et. al., 2019*).

Thirdly, the specific needs and rights of minors and children are too little recognized or foreseen in the development of the digital environment and the regulatory, state and commercial organizations that underpin it (Livingstone et al., 2015).

Another important aspect in the light of what has been discussed is that the GDPR imperatively imposes an obligation on business representatives who process personal data of minors to take appropriate measures to provide children with information about the future processing of their personal data: for what purposes is the personal data of a minor processed? To whom was or will (may be) disclosed the personal data of a minor?

All information must be provided in a concise, transparent, understandable and easily accessible form, in clear and simple language. For the presentation of information, minors are offered to use visualization, for example, videos, tables, symbols, etc. It is recommended to use various visualization tools in order for the minor to better understand how his or her personal data will be processed. In all cases, technologies for determining the location of minors must be avoided, since such data pose a particular risk to the safety of children. UNICEF noted in its report (2018) that physical privacy in the collection of personal data is violated in cases where the use of tracking, tracking or live streaming technologies may reveal the image, activity or location of the child. Also, various threats to the privacy of communication are associated with random access to records, conversations and messages. If there is no consent of minors in relation to the lawful processing of their data, the privacy, collection, storage and processing of personal data information of minors may be violated. The UNICEF report (2018) pays particular attention to the right of minors to privacy and the protection of personal data, the right to freedom of expression and access to diversity of information, the right to freedom from encroachment on reputation, the right to protection, the right to redress for violations and abuses of their rights – as specified in the UN Convention on the rights of the child (1989).

The third aspect is that business entities must avoid the formation of child profiles, and when this is inevitable, due to the specifics of the business, then profiling should be chosen by

the data subject or his legal representative through his active actions, for example, by placing a check mark on the section on the activation of profiling on the service provider's website. According to M. Macenaite (2017): *"The prohibition of profiling has the potential to diminish the commercial exploitation of children's data <...> happening through complex marketing, tracking and targeting systems used by many online service providers that monitor and monetize children's online behaviour and interactions"*. Profiling is understood as any form of automated processing of personal data consisting of the use of personal data to assess certain personal aspects relating to a natural person, in particular to analyse or predict aspects relating to that natural person's activities at work, economic situation, health status, personal interests, interests, reliability, behaviour, location or movement (*GDPR, 2018*) and should not be used for minors. In a general sense, decision-making only in an automated way means that decisions will be made by technological means, without any human intervention. Profiling is done when personal aspects of a person are evaluated to make predictions, even if no decision is made. If a company assesses a person's characteristics (such as age, gender or height) or divides them into certain categories, this means that the person is subject to profiling. Profiling and automated decision-making are common practices in various sectors, e.g., banking, finance, tax and healthcare. Using this method can be more effective, but less transparent. Therefore, both minors and their legal representatives must be informed in each case about all possible risks and negative consequences of profiling.

The fourth aspect, it is undeniable that the right of minors to privacy and the protection of personal data has been greatly influenced by the closure of schools due to the COVID-19 pandemic. In order to adapt to the pandemic situation, schools and teachers had to switch quickly to online and distance education. While it is clear that digital access and support measures are important not only for access to education, the privacy of minors must be maintained. Due to the pandemic, the increased use of educational technologies and the transition to online learning have also significantly increased data collection by companies that provide educational institutions with software that collect, process much more information and personal data about students and their private lives. Thus, businesses representatives, schools and education departments must implement various privacy and data protection regimes in the software, and take responsibility and accountability for personal data breaches. Schools should make appropriate decisions about educational programs and websites used in the school and inform the parents of students about such decisions. At the same time, lessons should be prepared for students on online privacy, digital citizenship, guidelines on how to behave and stay safe on the internet, and safe programs and websites for minors should be recommended (SolPriPa, 2019; Zimmerle, Wall, 2019).

Conclusions

The pandemic caused by the Covid-19 virus, development of information technologies, development of new data processing methods, prevalence of distance learning as a form of learning organization pose new challenges to the right of minors to private life and the implementation of ensuring the protection of personal data. The above processes have particularly highlighted the importance of the right of minors to data protection and privacy, and at the same time have led to a new look at the problems arising from the improper processing of personal data.

The right of minors to the protection and privacy of personal data is governed by the general legislation of the European Union and the Council of Europe. The right to privacy and protection of personal data are closely related, sometimes overlapping, but they are not identical

rights. Violation of personal data processing requirements also violates the right to privacy. The protection of the right to privacy is vital for the development of the minor child, therefore it is necessary to comply with the requirements of personal data protection processing and to assume responsibility and accountability for the data controllers when processing the data of minors.

Key measures to ensure the right of minors to data protection and privacy in the digital space: personal data of minors must be processed in accordance with the principle of transparency, free will, consent to the processing of data must be based on information, the information provided must be specific and unambiguous and must correspond to the maturity of the minor and be understandable to him or her. Depending on the state of the minor's residence and the age requirements, consent must be given by the minor himself or his legal representative. When processing data of minors, data controllers must follow the principle of data reduction, avoid technologies for determining the location of children and the formation of child profiles.

Also, to ensure the right of minors to data protection and privacy in the digital space, it is important to invest and take preventive measures: introducing new educational programs; preparing lessons for students on online privacy, digital citizenship; developing guidelines and measures on how to behave and stay safe on the internet, recommending the use of secure programs and websites for minors.

References

1. Article 29 Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP 251, 2018. Available at: file:///C:/Users/Dell/Downloads/20171013_wp251_en_9F78B0D5-E9A6-0271-6D40F3FE2DF49A1A_47742.pdf (Accessed: 20 May 2021).
2. Article 29 Data Protection Working Party, Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools), WP 160, 2009. Available at: https://ec.europa.eu/justice/article-29/documentation/opinion recommen dation/files/2009/wp160_en.pdf (Accessed: 20 May 2021).
3. Article 29 Data Protection Working Party, Working Document 1/2008 on the protection of children's personal data (General guidelines and the special case of schools), WP 147, 2008. Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2008/wp147_en.pdf (Accessed: 20 May 2021).
4. Charter of Fundamental Rights of the European Union, OL 7.6.2016, C 202/391. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12016 P/TXT&from=EN (Accessed: 9 April 2022).
5. Chaudron, S., Mascheroni, G. Rules of Engagement: Family Rules on Young Children' s Access to and Use of Technologies. In Danby et al. (eds.), *Digital Childhoods*, International Perspectives on Early Childhood Education and Development 22, Springer Nature Singapore Pte Ltd., 2018.
6. Council of Europe. Modernisation of the Data Protection "Convention 108". Available at: https://www.coe.int/en/web/portal/28-january-data-protection-day-factsheet_(Accessed: 12 May 2022).

7. European Convention for the Protection of Human Rights and Fundamental Freedoms, Council of Europe, Rome, 1950. Available at https://www.echr.coe.int/documents /convention_eng.pdf (Accessed: 11May 2022).
8. Data Global Hub. Children's personal data: GDPR. Available at: https://globaldatahub.taylorwessing.com/article/childrens-personal-data-gdpr (Accessed: 12 April 2022).
9. European Data Protection Supervisor, An official website of the European Union Available at: https://edps.europa.eu/data-protection/data-protection_en__(Accessed: 2 April 2022).
10. GDPR (General Data Protection Regulation). 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 Available at https://eur-lex.europa.eu/eli/reg/2016/679/oj. (Accessed: 9 April 2022).
11. Handbook on European data protection law, Luxembourg: Publications Office of the European Union, 2018. Available at: https://fra.europa.eu/sites/default/files/fra _uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf (Accessed: 3 Mayl 2022).
12. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas, Valstybės žinios. 1996. Nr. 63-1479. [The Law on Legal Protection of Personal Data of the Republic of Lithuania, Official Gazette, 1996, No. 63-1479].
13. Lietuvos Respublikos informacinės visuomenės paslaugų įstatymas, Valstybės žinios, 2006-06-10, Nr. 65-2380. [The law on information society services of the Republic of Lithuania, Official Gazette, 2006-06-10, No. 65-2380].
14. Lietuvos Respublikos Vaiko teisių apsaugos pagrindų įstatymas, Valstybės žinios, 1996-04-12, Nr. 33-807. [The law on the protection of the rights of the child of the Republic of Lithuania, Official Gazette, 1996-04-12, No. 33-807].
15. Livingstone, S., Mascheroni, G., Dreier, M., Chaudron, S. and Lagae, K. How parents of young children manage digital devices at home: The role of income, education and parental style, 2015. London: EU Kids Online, LSE.
16. Livingstone, S. Children: a special case for privacy? Intermedia, 2018, 46 (2), p. 18-23. Available at: http://eprints.lse.ac.uk/89706/1/Livingstone_Children-a-special-case-for-privacy_Published.pdf (Accessed: 19 May, 2022).
17. Livingstone, S. Stoilova, M., Nandagiri, R. Children's data and privacy online: Growing up in a digital age. An evidence review. London: London School of Economics and Political Science, 2019. Available at: http://eprints.lse.ac.uk/101283/1/Livingstone _childrens_data_and_privacy_online_evidence_review_published.pdf (Accessed: 5 April 2022).
18. Modernized Convention for the Protection of Individuals with Regard to the Processing of Personal Data, 128th Session of the Committee of Ministers, Elsinore, Denmark 17-18 May 2018 (Convention 108+), Available at https://www.europarl.europa.eu/meetdocs /2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf (Accessed: 17 April 2021).

19. M. Macenaite. From universal towards child-specific protection of the right to privacy online: Dilemmas in the EU General Data Protection Regulation. New media & Society, 2017, Vol. 19(5), p. 765–779.

20. Milkaite, I., Lievens, E. Children's Rights to Privacy and Data Protection Around the World: Challenges in the Digital Realm, 2018. Available at: https://ejlt.org/index.php/ejlt /article/view/674/912 (Accessed: 2 April 2022).

21. SolPriPa Project Guidelines. Asmens duomenų apsaugos gairės jaunuoliams [Personal Data Protection Guidelines for Youth] Solving Privacy Paradox Project, 2019. Available at https://vdai.lrv.lt/uploads/vdai/documents/files/02_%20SolPriPa%20Asmens%20duomenu%20apsaugos%20gaires%20JAUNIMUI%202019-11-06.pdf (Accessed: 19 April 2022).

22. Štareikė, E; Kausteklytė-Tunkevičienė, S. Pagrindinės duomenų subjekto teisės ir jų užtikrinimas pagal ES Bendrąjį duomenų apsaugos reglamentą [The main rights of the data subject and their enforcement in accordance with the EU General Data Protection Regulation]. Public Security and Public Order, 2018 (20), p. 293-312.

23. Štareikė, E; Kausteklytė-Tunkevičienė, S. Health data protection as a measure of realizing an individual's right to privacy. Public security of public order, 2021 (26), p. 236-249.

24. Štareikė, E. Assurance of the right to privacy and the protection of personal data in labour relations. Public security of public order, 2021, [t.] 26, p. 221-235.

25. The European Parliament resolution, dated July 6, 2011, on a comprehensive approach to the protection of personal data in the European Union (2011/2025(INI)). https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A52011IP0323 (Accessed: 16 April 2022).

26. UNICEF. Children's online privacy and freedom of expression: Industry toolkit, 2018. New York: UNICEF.

27. United Nations' Convention on the Rights of the Child, By General Assembly resolution 44/25, adopted 20 November 1989. Available at: https://www.ohchr.org/sites/default /files /crc.pdf (Accessed: 2 April 2022).

28. Universal Declaration of human rights. United Nations. Available at: šhttps://www.un.org/en/about-us/universal-declaration-of-human-rights (Accessed: 2 April 2022). EU Charter of fundamental rights.

29. Valstybinės duomenų apsaugos inspekcija. [State Data Protection Inspectorate, 2019]. Available at: https://vdai.lrv.lt/lt/naujienos/2019-m-lietuvos-gyventoju-tyrimas-apie-asmens-duomenu-apsauga-islaikyti-auksti-zinanciu-apie-savo-teises-ir-pareigas-asmens-duomenu-apsaugos-srityje-rodikliai (Accessed: 16 April 2022).

30. Valstybinės duomenų apsaugos inspekcija. Veiklos, dėl kurių turės būti atliekamas poveikio duomenų apsaugai vertinimas [State Data Protection Inspectorate, 2019]. Available at: https://vdai.lrv.lt/lt/naujienos/veiklos-del-kuriu-tures-buti-atliekamas-poveikio-duomenu-apsaugai-vertinimas (Accessed: 16 April 2022).

31. Valstybinė vartotojų teisių apsaugos tarnyba [State Consumer Rights Protection Authority]. Available at: https://www.vvtat.lt/veiklos-sritys/vartojimo-paslaugos/elektroniniu-rysiu-ir-informacines-visuomenes-paslaugos/81 (Accessed: 16 April 2022).

32. Zaeem, R. N., Barber, K. S. The Effect of the GDPR on Privacy Policies: Recent Progress and Future Promise. ACM Transactions on Management Information Systems, 2020, 12(1), p. 1-20.

33. Zimmerle, J., C, Wall, A., S. What's in a Policy? Evaluating the Privacy Policies of Children's Apps and Websites. Computers in the schools, 2019, Vol. 36(1), p. 38–47.