PERSONAL DATA
PROTECTION SERVICE

A Guide to Protecting Minors' Personal Data: Theory and Practice

A Guide to Protecting Minors' Personal Data: Theory and Practice

The publication was created by the Department of Planned Inspections of the Personal Data Protection Service and the Department of International Relations, Analytics, and Strategic Development.

Table of Contents

Foreword by the President of the Personal Data Protection Service

According to the UN “Convention on the Rights of the Child”, among other fundamental rights, a child has the right to privacy. The state is obliged to take all necessary legislative, administrative, and other measures to create conditions for the implementation and protection of children's rights.

The personal data of children and adolescents requires special protection. Article 7 of the new law "On Personal Data Protection" addresses the terms and conditions for giving consent to the processing of data about minors.[1] Therefore, the law recognizes and respects the basic rights and best interests of children and adolescents.

In the twenty-first century, the dangers of the digital environment that can affect the development of minors are increasing day by day. In the digital age, children's right to privacy needs to be protected to a high standard. With the development of new forms of communication, it is important to improve the standard of protection of basic rights. Additionally, awareness of risks is a crucial aspect of preventing the unlawful processing of data and raising awareness in this regard. To this end, the Personal Data Protection Service has developed a guide to the protection of minors' personal data, covering both practical and theoretical aspects.

The guide addresses various issues related to processing the personal data of minors, including the basics and principles of data processing. It outlines the rights of minors as data subjects and their implementation, such as the right to receive information, request information, rectify, update, add, block, erasure, and destroy data, withdraw consent, and transfer data, among others. The guide also covers the experience of the Personal Data Protection Service on specific issues and the international and national legal framework - International legal instruments and practices of processing minors' data, in particular, the protection of the right to privacy of minors in the legal system of the United Nations, the legal framework of the Council of Europe on the protection of personal data of minors, the standard of the European Court of Human Rights, etc.

I would like to express special thanks to Sofio Shamugia, head of the Department of the Planned Inspection of the Personal Data Protection Service, and Ana Tokhadze, head of the Department of International Relations, Analytics, and Strategic Development, as well as to each employee of these departments.

[1] The law will come into force on March 1, 2024, with the provisions on data protection impact assessment (Article 31), about the data protection officer (Article 32) becoming effective on June 1, 2024.

I think the guide will contribute to the development of Georgian personal data law and the culture of data protection, which represents one of the primary focuses of the supervisory body for personal data protection.

Professor, Dr. Dr. Lela Janashvili

President of the Personal Data Protection Service of Georgia

Professor at Ivane Javakhishvili Tbilisi State University, Doctor of Law

Visiting Professor at the Autonomous University of Barcelona

Introduction

Modern digital technologies have profoundly transformed the world. Minors are increasingly engaging in the digital space, which has become an inseparable part of their lives, posing certain risks regarding the privacy of children and the protection of personal data. The legal framework in Georgia pertaining to personal data protection does not explicitly outline procedures for safeguarding children's personal data in the digital environment. Hence, it is crucial to reference international standards to establish suitable guarantees.

The aim of the paper is to examine the optimal international standards concerning the rights of minors in the digital environment and beyond, and to align them with national legislation. It focuses on the principles and fundamentals of data processing, the child's rights to personal data protection, and individual considerations related to the concept of the "child's best interest." A key focus of the Personal Data Protection Service is assessing the lawfulness of processing minors' personal data and implementing appropriate measures in response to identified challenges. Hence, it is noteworthy that both in 2022 and 2023, "On the approval of the plan for planned inspections of the lawfulness of personal data processing," minors were delineated among other target groups according to the orders issued by the President of the Personal Data Protection Service, specifically No. 01/23 dated April 7, 2022, and No. 01/20 dated January 31, 2023. The Service consistently endeavors to disseminate the best international practices for protecting children's rights and establishing effective standards, a pursuit particularly pertinent during the implementation of the new law on "personal data protection." This guide also serves as an academic contribution, encapsulating the fundamental aspects of processing minor data and significant decisions made by the Personal Data Protection Service.

The document holds a recommendatory nature, thus, the Personal Data Protection Service retains the prerogative to render decisions that may differ from the perspectives outlined in the paper, considering the unique circumstances of individual cases.

1. The Minor as a Data Subject and the National Legal Framework

1.1. National Legislation on Personal Data Protection

The law governing the protection of personal data is evolving rapidly alongside technological advancements, highlighting the growing significance of individuals' informational self-determination. Awareness regarding personal data protection is integral to the unrestricted development of an individual, rooted in the capacity for self-directed growth, decision-making, and choice. According to legislation in the European Union and the Council of Europe, "personal data" encompasses any information relating to an identified or identifiable natural person, whose identity either is known or can be ascertained based on supplementary information.[2] Under EU legislation, data protection rules primarily benefit natural persons.[3] The key components of the concept of personal data include "any information"; "related to"; "identified or identifiable"; and "natural person".[4] The phrase "any information" underscores the legislator's intent to provide a broad definition of personal data. In this context, the German Constitutional Court elucidated in 1983 that "in the realm of automatic data processing, no information is insignificant".[5] Any information pertaining to an individual may fall under a special category.[6] Hence, personal data encompasses any information, irrespective of whether it pertains to a person's personal life, employment, economic or social circumstances, or their capabilities.[7] Information can be either "objective," encompassing the unalterable attributes of the data subject, or "subjective," comprising opinions and assessments.[8] It doesn't need to be accurate, validated, or exhaustive.[9] What's crucial is that the information is associated with a particular individual. According to the opinion of the Article

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4/5/2016, 1-88 art. 4 (1) (Hereinafter - "GDPR"); Council of Europe, Modernized Convention for the Protection of Individuals with Regard to the Processing of Personal Data (Convention 108+; CM/Inf (2018) 15-final), 18/05/2018, Article 2 (a).

[3] GDPR, Article 1.

[4] The EU Agency for Fundamental Rights and Council of Europe, Handbook on European Data Protection Law, 2018, 96.

[5] German Federal Constitutional Court, 1 BvR 209/83, 269/83, 362/83, 420/83, 440/83, 484/83, 15 December 1983, margin number 150.

[6] Commission of the European Communities, COM (90) 314, final, 13 September 1990, 19.

[7] WP29, Opinion 4/2007 on the concept of personal data, 20 June 2007, 6.

[8] Ibid, "especially the latter type of information constitutes a significant part of the processing in sectors such as banking, insurances or employment".

[9] Ibid.

29 Working Party,[10] the precursor to the "European Data Protection Board",[11] "the information, by its content, purpose, or effect, must be connected to a specific person".[12] According to the EU "General Data Protection Regulation", an identifiable natural person is someone who can be directly or indirectly identified using an identifier such as a name, personal number, location information, online identifier, or one or more factors related to physical, psychological, genetic, mental, economic, cultural, or social characteristics.[13] It's important to note that, according to Article 8 of the Universal Declaration of Human Rights,[14] data protection is a universal right and is not restricted to citizens of specific countries.[15]

The preamble of the "General Data Protection Regulation" of the European Union anticipates a distinct regulation regarding the processing of minors' data. Minors are entitled to special personal data protection, as they might have limited awareness of the risks, consequences, legal protections, and their rights concerning the processing of personal data.[16] Special safeguards should be in place for the utilization of minors' personal data for marketing purposes, creating an individual or user profile, and gathering personal data associated with minors during the utilization of services directly targeted at them. It is important to note that the consent of the parent or legal representative of the minor is not required in cases of directly offering preventive or counseling services to minors. Minors constitute a vulnerable group, warranting an elevated standard of protection for their rights.[17] Furthermore, in accordance with the "General Data Protection Regulation," due to the specific protection requirements of minors, any information targeted at them must be conveyed clearly, simply, and comprehensibly. This aligns with the principles of fairness and legality, ensuring that data is processed fairly and lawfully, without compromising the dignity of the data subject.[18]In this context, it is worth mentioning that in 2013, the "Organization for Economic Co-operation and Development" ("OECD") endorsed guidelines for privacy protection. These guidelines emphasize that given the unique and particular circumstances of children, it is the responsibility of states to furnish

[10] The European Data Protection Board (EDPB) is established under Article 68 of the GDPR as an independent EU body which contributes to the consistent application of data protection rules throughout the EU, and promotes cooperation between the EU's data protection authorities. The EDPB is composed of representatives of the national data protection authorities, and the European Data Protection Supervisor (EDPS).

[11] WP29, Opinion 4/2007 on the concept of personal data, 20 June 2007, 10 ff <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf>, [18.08.2023].

[12] CJEU, Nowak, 20 December 2017, margin number 35.

[13] General Data Protection Regulation, GDPR, Recital 14 sentence 1.

[14] Convention on the rights of the child, international contract and agreement of Georgia, 1948, Article 8.

[15] General Data Protection Regulation, GDPR, Recital 14.

[16] General Data Protection Regulation, GDPR, Recital 38.

[17] Ibid.

[18] Law of Georgia "On Personal Data Protection", date of adoption: 28/12/2011, subparagraph "a" of Article 4, <https://matsne.gov.ge/ka/document/view/1561437?publication=31>, [10.08.2023].

them with comprehensive information to ensure their safety online and enable them to harness the Internet to their advantage.[19]

The national legislative framework for personal data protection aligns with the international legal definition of the concept of personal data. The Georgian model of personal data protection mirrors the European approach, whereby both domestic and international regulations govern the operation of the law across all sectors—private, public, and law enforcement agencies. In Georgia, personal data protection is governed by a single legislative act—the Law of Georgia "On Personal Data Protection," initially adopted on December 28, 2011 (first edition).[20] In order to align the existing legislation in the field of personal data protection with European standards, fulfill international obligations, establish internationally recognized principles, and address challenges within public and private institutions as well as law enforcement agencies, Georgia adopted the Law of Georgia "On Personal Data Protection" on June 14, 2023,[21] This law introduces new legal guarantees for personal data protection, defines rules, and addresses various issues, including the processing of personal data of minors.[22]

In the original edition of the Law of Georgia "On Personal Data Protection," specific provisions regarding the processing of personal data of minors were absent. However, the new version of the law significantly enhances the rights of data subjects and expands guarantees for their protection. It introduces special regulations concerning the processing of personal data of minors. Particularly, Article 7 outlines the procedure and conditions for obtaining consent for processing data about minors. Moreover, when processing data about a minor, data controller is obligated to consider and safeguard the best interests of the minor.[23] Additionally, one of the justifications for the permissibility of video surveillance is the protection of minors, including safeguarding them from harmful influences.[24] Under the new law, one of the exceptions to the obligation to cease data processing upon request by the data controller is the overriding interest in protecting the rights of minors.[25] A legislative novelty is that the data controller is mandated to provide information to the data subject, particularly if the data subject is a minor, in a simple and understandable language.[26] Additionally, committing an administrative offense by a minor is considered one of the mitigating circumstances of responsibility,[27] while processing a minor's

[19] OECD Privacy Framework, 2013, 31.

[20] Law of Georgia "On Personal Data Protection", date of adoption: 28/12/2011.

[21] Law of Georgia "On Personal Data Protection", date of adoption: 14/06/2023,<https://matsne.gov.ge/document/view/1561437?publication=30>, [10.08.2023].

[22] 2022 Activity Report of the Personal Data Protection Service of Georgia, 197-202.

[23] Law of Georgia "On Personal Data Protection", date of adoption: 14/06/2023, Article 7.

[24] Ibid., Article 10.

[25] Ibid., subparagraph "g" of the second paragraph of Article 17.

[26] Ibid., Paragraph 5 of Article 24.

[27] Ibid., subparagraph "b" of the first paragraph of Article 61.

data in contravention of the law's requirements is deemed an aggravating circumstance of responsibility.[28]

1.2. An overview of the Sectoral National Legislation

The purpose of the legislative act regulating the protection of children's rights in Georgia, the Code "on the Rights of the Child," is to ensure the well-being of children by promoting the effective implementation of the Constitution of Georgia, the Convention on the Rights of the Child, its additional protocols, and other international legal acts recognized by the state.[29] The Code defines the basic rights and freedoms of children, establishes the legal foundation for their protection, and ensures the functioning of the support system.[30] For the purposes of the Code, a child is defined as a person under the age of 18, encompassing all minors regardless of different characteristics, which are directly related to the right to equality.[31]

Article 9 of the Code of Children's Rights provides for the child's right to private and family life. It states that the child has the right to have personal space and to conduct personal correspondence. Any illegal restriction of the child's right to private and family life, including unjustified and illegal interference in their personal space, family life, or personal correspondence, is not allowed.[32] The Code does not prohibit the processing of a child's personal data for purposes such as health protection, education, and social protection. However, such processing must be based on the best interests of the child and must comply with Georgian legislation.[33] The definition of the best interest of the child provided in the Code is not exhaustive, allowing for subjective assessment.[34] In light of the development of modern technologies, the following rights are also relevant in the context of the processing of minors' personal data, as stipulated by the Code of Children's Rights: the right to life and personal development of the child,[35] the right to education,[36] and the rights to freedom of opinion, information, mass media, and the Internet.[37]

In relation to minors, when discussing personal data protection, it is important to mention the "Juvenile Justice Code." This code establishes "administrative and criminal liability of minors,

[28] Ibid., subparagraph "g" of Article 62.
[29] Law of Georgia, Code on the Rights of the Child, 20/09/2020, Article 1, <https://matsne.gov.ge/document/view/4613854?publication=4>, [10.08.2023].
[30] Ibid., the first part of Article 2.
[31] Kiladze, S., Turava, P., Guiding Commentaries of the Code on the Rights of the Child, 2021, 47.
[32] The Code on the Rights of the Child, Article 9.
[33] Kiladze, S., Turava, P., Guiding Commentaries of the Code on the Rights of the Child, 2021, 278.
[34] Ibid., 43.
[35] The Code on the Rights of the Child, Article 6.
[36] Ibid., Article 10.
[37] Ibid., Article 14.

the features of administrative offense proceedings involving minors, and special procedures for the execution of punishment and other measures."[38] The purpose of the Code is "to protect the best interests of minors in the justice process, facilitate the resocialization and rehabilitation of minors in conflict with the law, safeguard the rights of minor victims and witnesses, prevent secondary victimization and re-victimization of minor victims, prevent new crimes, and uphold law and order."[39]

Article 13 of the Code guarantees the minor's right to privacy. According to the same article, "the protection of the personal life of a minor is ensured at any stage of juvenile justice. Information about the conviction and administrative responsibility of a minor is not public. It is not allowed to disclose and publish the personal data of a minor, except for the cases stipulated by the Law of Georgia "On Personal Data Protection."[40] In the context of juvenile justice, the inviolability of personal life comprises two crucial components: a) The state prohibits the dissemination of information about a child in conflict with the law that would enable their identification. b) During television reports, measures should be taken to prevent the identification of teenagers by appearance, ensuring that those "identified as criminals" do not encounter difficulties with integration and resocialization in society. The right to privacy is closely intertwined with other rights, including the preservation of identity, the presumption of innocence, protection of the genuine interests of the child, and the dignity and inviolability of the child. All these elements are fundamental to a child's healthy emotional, spiritual, and physical development.[41]

1.3. Separate Elements of Minor Data Processing

Minors rapidly embrace new opportunities and emerge as independent users of digital technologies.[42] Given that minors are vulnerable groups within society, special attention must be given to the processing of their data. Data processing encompasses any action or series of actions involving personal data or a dataset, conducted through automated or other means.[43] When processing data of minors, data controller is obligated to establish special systems and adhere to the principles of data protection. It is particularly crucial to have legal justifications for the processing.[44] Data processing is deemed lawful if it adheres to the law, serves a

[38] Juvenile Justice Code, Part 1 of Article 1.
[39] Ibid., Part 2 of Article 1.
[40] Ibid., Article 13.
[41] Shalikashvili M., Mikanadze G., Juvenile Justice (Manual), 2016, 86-87.
[42] ICO, Children's Data and Privacy Online, 4.
[43] The EU Agency for Fundamental Rights and Council of Europe, Handbook on European Data Protection Law, 2018, 113-116.
[44] ICO, Children and the GDPR, 2018, 1.

legitimate purpose, and is necessary and proportionate in a democratic society.[45] According to the EU General Data Protection Regulation, processing the personal data of a minor is lawful if the minor is at least 16 years old; Processing the personal data of someone under 16 is only lawful if consent is given or if processing is authorized by a parent or legal representative. Member states have the authority to establish a lower age limit by law, but not less than 13 years.[46] Determining the age limit is crucial and depends on various factors. Primarily, it relates to the child's capacity to consciously understand their own rights. However, if it is evident that the child is acting against their own best interests, they may not be considered competent.[47] In the process of national legal reform, the right of a minor to independently express their will through consent was considered. Similar to European regulations, this right is tied to the age limit, which is also set at 16 years.[48] Additionally, the general comment of the UN Committee underscores the right to hear the child's opinion. According to this comment, states must guarantee children's freedom of expression, allowing them to form opinions on all matters that concern them.[49]

1.4. Best Interest of the Child

The principle of protecting the best interests of children is acknowledged and reinforced by numerous legal acts, both at the national,[50] and international levels.[51] In the context of personal data protection, the best interests of minors are safeguarded by the 1989 Convention on the Rights of the Child ("CRC"). According to the CRC, whenever actions are taken by public or private social welfare institutions, courts, administrative or legislative bodies concerning children, the best interests of the child must be the primary consideration.[52] The definition of the best interests of the child is dynamic and adaptable to adequately address all potential cases and challenges related to children.[53] When determining the best interest of the child, it is crucial to first identify the specific circumstances that make the child's situation unique. In assessing the best interest, the following elements should be taken into account: the opinion

[45] Kuner Ch., Bygrave L. A., Docksey Ch., The EU General Data Protection Regulation (GDPR), a Commentary, Oxford University Press, 2020, 314.

[46] GDPR, ART. 8.1.

[47] See the official website of the UK Personal Data Protection Authority: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-dataprotection-regulation-gdpr/children-and-the-gdpr/what-rights-do-children-have/>, [10.08.2023].

[48] Law of Georgia "On Personal Data Protection", date of adoption: 14/06/2023, Article 7.

[49] General Comment No. 12 (2009) The Right of the Child to be Heard, §§20-21.

[50] The Code on the Rights of the Child, Law of Georgia, 27/09/2019.

[51] Convention on the Rights of the Child, International contract and agreement of Georgia, 1948.

[52] UN, Convention on the Rights of the Child, Adopted and opened for signature, ratification and accession by General Assembly resolution 44/25 of 20 November 1989, Article 3.1

[53] Kiladze, S., Turava, P., Guiding Commentaries of the Code on the Rights of the Child, 2021, 44.

of the child; the child's identity; providing a family environment and maintaining relationships; child care, protection, and security; considering vulnerability; the right to protect the child's health; and the child's right to education.[54] The concept of the best interest of a minor entails the comprehensive and effective realization of all rights outlined by the convention, ensuring the complete development of the minor and safeguarding their dignity. Full development encompasses physical, mental, spiritual, moral, psychological, and social aspects.[55]

The obligation to prioritize the best interests of the child is three-dimensional and includes a substantive right, a basic legal principle, and a procedural norm. This implies: the right of a minor to have his best interests evaluated and considered to be preferred when various interests are considered for a decision on a specific issue; The decision-making process related to a minor should include an assessment of the possible impact (positive or negative) of this decision on the relevant child or children.[56] Assessment and determination of the best interests of the child require procedural guarantees.[57]

The concept of the best interests of the child was explored by the predecessor Article 29 Working Party of the European Data Protection Board ("EDPB")[58] in a 2009 opinion,[59] which stated that the best interests of the child must be protected by all those involved in decisions relating to children. This is based on the fact that a person who has not yet reached physical and psychological maturity needs more protection, compared to other age groups. Jurisprudence confirms that the best interest of the child seen from the "parent's eyes" is not always the same as the best interest of the child,[60] which, in the modern era, may be reflected

[54] Data Protection Commission of Ireland, Children Front and Centre, Fundamentals for Child-Oriented Approach to Data Processing, December 2020, 19.

[55] UN General Comment No. 14 (2013) On the Right of the Child to Have His or Her Best Interests Taken as Primary Consideration, §§4-5.

[56] Digital Futures Commission, Child Rights Impact Assessment, a Tool to Realize Children's Rights in the Digital Environment, 2021, 8-9.

[57] UN General Comment No. 14 (2013) On the Right of the Child to Have His or Her Best Interests Taken as Primary Consideration, § 6.

[58] The European Data Protection Board (EDPB) is established under Article 68 of the GDPR as an independent EU body which contributes to the consistent application of data protection rules throughout the EU, and promotes cooperation between the EU's data protection authorities. The EDPB is composed of representatives of the national data protection authorities, and the European Data Protection Supervisor (EDPS).

[59] Opinion 2/2009 on the Protection of Children's Personal Data (General Guidelines and the Special Case of Schools).

[60] "In 2017, a 16-year-old minor took legal action against their parent for posting their photo on a social network without consent. The court ruled in favor of the minor, ordering the parent to delete the photo. Failure to comply would result in a fine of 10,000 euros as a sanction. Similarly, in 2016, an Australian teenager sued their parents

in the different views of parents and minor children, including in the context of the protection of personal data of minors in the digital environment.[61]

2. General Overview of Data Processing Principles

The right to protection of children's private and family life in the digital environment encompasses safeguarding their personal data and respecting the privacy of their correspondence and personal communications.[62] The protection of children's private life extends to their physical and mental integrity, decision-making autonomy, identity, informational, and physical or spatial privacy.[63] To uphold the inviolability of a child's privacy, it is crucial to adhere to the principles of data processing when handling their data and to process it in their best interests[64] while also considering national legislation and the EU's "Basic Data Protection Regulation." This chapter discusses the six main principles of data protection:

- Fairness, lawfulness and transparency;
- Specified, explicit, and legitimate purpose;
- Data minimisation;
- Authenticity and Accuracy;
- Storage limitation;
- Data Security;

for posting up to 500 "shameful" photos on social media over the past 7 years without their consent". Shudra T., "Protecting the Personal Data of Minors in the Digital Environment with Different Expectations of Parents and Children," Journal of Personal Data Protection Law, No. 1, 2023, Footnote. 10, 109, Reference: Goshadze K., Legal Implications of "Shattering", International Journal of Law: "Law and World ", №15, Vol. 6, Issue 2, 2020, 5.

[61] Shudra T., "Protecting the Personal Data of Minors in the Digital Environment with Different Expectations of Parents and Children," Journal of Personal Data Protection Law, №1, 2023, 109.

[62] Committee of Ministers, Guidelines to Respect, Protect and Fulfil the Rights of the Child in the Digital Environment, Recommendation CM/Rec(2018)7, §26, <https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a>, [10.08.2023].

[63] The Special Rapporteur on the Right to Privacy, Joseph A. Cannataci, Artificial Intelligence and Privacy, and Children's Privacy, Report, §71, <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G21/015/65/PDF/G2101565.pdf?OpenElement>, [10.08.2023].

[64] Committee of Ministers, Guidelines to Respect, Protect and Fulfil the Rights of the Child in the Digital Environment, Recommendation CM/Rec(2018)7, §29, <https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a>, [10.08.2023].

2.1. Fairness, Lawfulness and Transparency Principle

The new law of Georgia "On Personal Data Protection" incorporates the principle of lawfulness, fairness, and transparency, stipulating that data must be processed lawfully, fairly, transparently for the data subject, and without infringing upon their dignity.[65]

2.1.1. Lawfulness

The lawful processing of personal data necessitates that data should only be processed when there is a relevant legal basis[66] and all legal requirements are fulfilled,[67] irrespective of whether the data pertains to a child or an adult.[68] Processing operations must fully comply with legal requirements.[69] Primarily, for processing to be deemed lawful, it must adhere to Article 6 of the EU General Data Protection Regulation, which mandates any processing operation to satisfy at least one of the six legal grounds enumerated in an exhaustive list:[70] a) Consent of the data subject; b) Execution of the contract or taking certain measures before signing it; c) Fulfillment of legal obligation; d) Protection of the vital interests of the data subject or other natural person; e) Performing tasks in the field of public interest or exercising official authority; f) Legitimate interests of data controller or other parties, provided that these interests are not outweighed by the interests or fundamental rights and freedoms of the data subject.[71]

Considering the above, personal data collection and processing operations are only permissible when there is a legitimate basis for processing, such as consent. If personal data collection occurred due to unauthorized access, the processing would be unlawful, thus violating the

---

[65] Law of Georgia "On Personal Data Protection", date of adoption: 14/06/2023, Subparagraph "a" of the First Paragraph of Article 4.

[66] Adv. Prashant Mali, GDPR Articles with Commentary & EU Case Laws, 15.

[67] Christopher Kuner, Lee A. Bygrave, Christopher Docksey, The EU General Data Protection Regulation (GDPR), A Commentary, Oxford University Press, 2020, 314.

[68] Data Protection Commission, Irish DPA, Children Front and Centre, Fundamentals for a Child-Oriented Approach to Data Processing, 2021, 22 <https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf>, [10.08.2023].

[69] Sanjay Sharma, PhD with research associate Pranav Menon, 2020, 126.

[70] GDPRhub, GDPR commentary, <https://gdprhub.eu/index.php?title=Article_5_GDPR#Lawful>, [10.08.2023].

[71] Data Protection Commission, Irish DPA, Children Front And Centre, Fundamentals for a Child-Oriented Approach to Data Processing, 2021, 22 <https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf>, [10.08.2023].

principle of lawfulness.[72] Moreover, data processing must serve a legitimate purpose, be necessary, and proportionate in a democratic society.[73]

2.1.2. Fairness

Fairness is a comprehensive principle demanding that personal data are not processed to the detriment of the data subject, in a discriminatory manner, or in a manner that is unexpected or misleading.[74] According to this principle, obtaining or otherwise processing data through unfair means, misleading practices, or without the knowledge of the data subject is prohibited.[75] The purpose of this principle is to safeguard the interests of the individual, which holds particular importance, especially in the case of children.[76] It's crucial that the data subject is informed about the processing of their personal data, including how the data will be collected, stored, and used. However, in certain cases, processing is permitted by law and deemed fair, regardless of the data subject's knowledge and preferences.[77]

The determination of the fairness of a processing operation must be contextual.[78] One of the guidelines from the European Data Protection Board (EDPB)[79] provides a non-exhaustive list of certain elements of fairness that must be adhered to when processing personal data. Important elements of fairness include the expectation,[80] of the data subject regarding the

---

[72] Adv. Prashant Mali, GDPR Articles with Commentary & EU Case Laws, 15.
[73] Kuner Ch., Bygrave L. A., Docksey Ch., The EU General Data Protection Regulation (GDPR), A Commentary, Oxford University Press, 2020, 314.
[74] EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, 2020, §69, <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf>, [18.08.2023].
[75] Kuner Ch., Bygrave L. A., Docksey Ch., The EU General Data Protection Regulation (GDPR), A Commentary, Oxford University Press, 2020, 314.
[76] Information Commissioner's Office (ICO), Children and the GDPR, 2018, 12, <https://ico.org.uk/media/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/children-and-the-uk-gdpr-1-0.pdf>, [18.08.2023].
[77] Eduardo Ustaran, CIPP/E, Partner, Hogan Lovells, European Data Protection Law and Practice, Second Edition, 2019, 128.
[78] GDPRhub, GDPR commentary, <https://gdprhub.eu/index.php?title=Article_5_GDPR#Lawful>, [18.08.2023].
[79] EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, 2020, <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf>, [18.08.2023].
[80] See, Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Convention 108, Children's Data Protection in Education Systems: Challenges and Possible Remedies, 2019, 12, <https://rm.coe.int/t-pd-2019-06final-eng-report-children/1680a01b47>, [18.08.2023].

reasonable use of their data, as well as the right to protection from discrimination or exploitation based on a certain psychological state. According to the EDPB definition, for processing to be considered "fair", deceptive processing of data is not permitted, and each choice must be presented objectively and neutrally, avoiding misleading or manipulative language or design.[81] Special attention should be given to clarity of language when providing information to children.[82]

2.1.3. Transparency

The principle of transparency is intricately linked to the principle of fair data processing. Before the implementation of the GDPR, transparency requirements were considered an integral component of the concept of fairness.[83] According to the principle of transparency, individuals should have clarity regarding the collection, use, disclosure, or other processing of personal data related to them.[84] Additionally, under the GDPR, if individuals receive information from an organization about the use of their personal data, it should be presented in a concise, transparent, understandable, and easily accessible format, using clear and simple language. Ensuring clarity of information is especially crucial when it is communicated to a child.[85] According to the definitions outlined by the Working Party on Article 29, transparency is regarded as an independent right applicable to both children and adults.[86] This signifies that children possess the right to be informed about the processing of their personal data,[87] irrespective of the legal basis of the processing, even in cases where a parent or guardian has consented to the processing of their own personal data on behalf of the child.[88]

---

[81] GDPRhub, GDPR commentary, <https://gdprhub.eu/index.php?title=Article_5_GDPR#Lawful>, [18.08.2023].
[82] Kuner Ch., Bygrave L. A., Docksey Ch., The EU General Data Protection Regulation (GDPR), a Commentary, Oxford University Press, 2020, 315.
[83] Ibid., 314.
[84] GDPR, Recital 39.
[85] Data Protection Commission, Irish DPA, Children Front and Centre, Fundamentals for a Child-Oriented Approach to Data Processing, 2021, 27.
[86] Article 29 Working Party Guidelines on transparency under Regulation 2016/679, 2018, §14, <https://ec.europa.eu/newsroom/article29/items/622227/en>, [18.08.2023].
[87] See, Information Commissioner's Office (ICO), Children and the GDPR, 2018, 38, <https://ico.org.uk/media/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/children-and-the-uk-gdpr-1-0.pdf>, [18.08.2023].
[88] Data Protection Commission, Irish DPA, Children Front And Centre, Fundamentals for a Child-Oriented Approach to Data Processing, 2021, 27, <https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf>, [18.08.2023].

Tailoring transparency information to the appropriate audience is crucial.[89] Therefore, it is insufficient to present information to children in complex, legalistic, vague, or colloquial language.[90] The principle of transparency mandates that when children are the intended audience of data controllers or when their products or services are predominantly used by children, all information and communication should be communicated in clear and simple language[91] or through easily understandable means.[92] Visual techniques, such as animations, pictograms, infographics, photos, and videos,[93] can be employed to captivate children's interest effectively.[94] When choosing suitable measures, it's essential to consider the specific service, the child's age, and developmental stage. It's advisable for data controllers to utilize the format that aligns most with the service provided. For instance, if they operate on a video sharing platform, using video would be a more fitting medium to communicate information to children than images or text.[95]

2.1.4. International Judicial Practice

The European Court of Human Rights has consistently affirmed that, according to the first paragraph of Article 8 of the European Convention on Human Rights, the processing of personal data can, in specific circumstances, constitute interference with the data subject's right to respect for private life.[96] For such interference to be deemed justified, it must comply with the law (Paragraph 2 of Article 8 of the Convention), which may be associated with the

[89] Morgan A., The Transparency Challenge: Making children aware of their data protection rights and the risks online, Volume 23, No.1, 2018, 3, <https://www.dataprotection.ie/sites/default/files/uploads/2019-02/TransparencyChallenge.pdf>, [18.08.2023].

[90] Data Protection Commission, Irish DPA, Children Front and Centre, Fundamentals for a Child-Oriented Approach to Data Processing, 2021, 27.

[91] See. Ibid., 29.

[92] Article 29 Working Party Guidelines on transparency under Regulation 2016/679, 2018, §§14-15, <https://ec.europa.eu/newsroom/article29/items/622227/en>, [18.08.2023].

[93] Morgan A., The Transparency Challenge: Making Children aware of their Data Protection Rights and the Risks Online, Volume 23, No.1, 2018, 3, <https://www.dataprotection.ie/sites/default/files/uploads/2019-02/TransparencyChallenge.pdf>, [18.08.2023].

[94] Information Commissioner's Office (ICO), Children and the GDPR, 2018, 38, <https://ico.org.uk/media/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/children-and-the-uk-gdpr-1-0.pdf>, [18.08.2023].

[95] Data Protection Commission, Irish DPA, Children Front And Centre, Fundamentals for a Child-Oriented Approach to Data Processing, 2021, 29, <https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf> [18.08.2023].

[96] See Case of S. and Marper v. the United Kingdom, [GC], [2008] ECTHR App. Nos. 30562/04 and 30566/04; case of L.B. v. Hungary, [GC], [2023] ECTHR App. No. 36345/16.

requirement of lawful processing. This legal framework should be predictable in terms of its consequences. In the case "Rotaru v Romania",[97] the court observed that for foreseeability, domestic legislation should establish limits on the authority's powers: the law should delineate the types of information that can be processed; categories of individuals from whom information may be collected; circumstances under which such measures may be taken; individuals who can access the data; and data retention periods.[98]

In the case of "Bara",[99] the Court of Justice of the European Union determined that, in accordance with the requirement of fair processing of personal data, a public institution must inform the data subjects about the transfer of their personal data to another similar body.[100]

In the case of "M.S.",[101] the court observed regarding the requirement of transparency that operations related to personal data, such as the transfer of data to third parties, must align with the reasonable expectations of the data subject. The court noted that the subsequent use of the contested data served a different purpose that exceeded the applicant's expectations, leading to the conclusion that there had been an interference with the applicant's right to private life.[102]

2.1.5. Practice of the Personal Data Protection Service

- *The teacher of one of the public school*

Every decision concerning minors should be made considering the best interests of a child. The persons caring for children, including teachers, perform the special role in the proper exercise of the right to privacy. Having regard to the above mentioned, on the basis of a request, the Personal Data Protection Service of Georgia examined the lawfulness of taking photos of public school students by the teacher of the same school and the disclosure of the photo(s) by him/her. According to the information obtained by the Service from publicly

[97] Case of Rotaru v Romania, [GC], [2000] ECTHRApp. No. 28341/95.
[98] Kuner Ch., Bygrave L. A., Docksey Ch., The EU General Data Protection Regulation (GDPR), a Commentary, Oxford University Press, 2020, 313.
[99] CJEU, Case C- 201/ 14, Bara [2015], §34.
[100] Kuner Ch., Bygrave L. A., Docksey Ch., The EU General Data Protection Regulation (GDPR), a Commentary, Oxford University Press, 2020, 313.
[101] Case of M.S. v. Sweden, [1997] ECHR App. No. 74/1996/693/885.
[102] Kuner Ch., Bygrave L. A., Docksey Ch., The EU General Data Protection Regulation (GDPR), a Commentary, Oxford University Press, 2020, 313.

available sources, it was revealed that the school teacher had taken the photos of minors kneeling/ squatting during the lesson and sent them to their parents.

As a result of the probe into the lawfulness of data processing by the school teacher, the Service stated, that the public school teacher had taken two photographs of students. In particular, one photo depicted those pupils, who had come prepared for the lesson, sitting at their desks, and in another photo there were captured so called "squatting" students, who had not learnt the lesson. According to the explanation provided by the public school teacher, capturing the situation of punishing students in a photo and sending the said photo to the parents was conditioned by the learning objectives. In particular, he wanted to inform the parents about their children's academic performance, so that they also could feel responsibility. He was sure that such a measure would be the source of motivation for students to learn better. The teacher also pointed out that the mentioned measure had paid off and the students started to improve their learning performance. It should be noted that the students in the photo, circulated in the media, made the impression as if they were in a "kneeling" position. Regardless of whether the children were in the "squatting" or "kneeling" position, in both cases their photograph, given the full context of the photo taken and sent to the parents, emphasized their difference from the students who came to the class prepared. In addition, taking into account the factor that the mentioned condition of students was associated with their poor academic performance, both being in "squatting" and "kneeling" positions were perceived as the violation of dignity. The infringement of a minor's dignity was thus singled out as a counterbalance to the educational objectives set by the educator, which, in turn, constituted the threat of being the victim of oppression of children, so called "bullying", their discrimination and ill-treatment. Giving consideration to the above mentioned, the Service established that when processing the data of students, who were not prepared for the lesson, the school teacher did not observe the principle of data processing without violating the dignity of the data subject. Therefore, the school teacher was held liable for the administrative offence pursuant to Paragraph 1 of Article 44 of the Law of Georgia on Personal Data Protection.

2.2. Specified, Explicit, and Legitimate Purpose

Purpose limitation stands as one of the cornerstone principles in European data protection law.[103] Determining the purpose of any processing operation serves as the initial stage in applying data protection legislation and formulating data protection safeguards. Moreover, establishing the objective is essential as a precursor to defining other requirements. The principle of purpose limitation sets boundaries within which personal data collected for a specific purpose can be processed and subsequently utilized.[104] This principle implies that data should only be collected for specific, explicit, and legitimate purposes.[105] Personal data collected for one purpose cannot be freely used[106] for another purpose.[107] If further data processing is contemplated, the data controller must first ensure that the intended processing aligns with the original purpose. Whether the new purpose is consistent with the original purpose must be assessed according to the criteria outlined in Article 6, paragraph 4 of the GDPR.[108]

2.2.1. Accuracy

The specific purpose implies that, in any case, the purpose must be precisely and fully identifiable in advance,[109] no later than the beginning of the collection of personal data. This is necessary to determine what kind of processing a particular purpose involves. Additionally, a specific purpose allows for the assessment of its compliance with the law and the data protection mechanisms used.[110] Personal data must be collected for specific purposes.

[103] Handbook On European Data Protection Law, 2018, 140 <https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_ka.pdf>, [18.08.2023].
[104] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, 2013, 4, <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf>, [18.08.2023].
[105] Kuner Ch., Bygrave L. A., Docksey Ch., The EU General Data Protection Regulation (GDPR), a Commentary, Oxford University Press, 2020, 315.
[106] GDPRhub, GDPR commentary, <https://gdprhub.eu/index.php?title=Article_5_GDPR#Lawful>, [18.08.2023].
[107] Law of Georgia "On Personal Data Protection", date of adoption: 14/06/2023, Subparagraph "b" of the first paragraph of Article 4.

[108] EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2, 2020, §71, <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf>, [18.08.2023].
[109] Kuner Ch., Bygrave L. A., Docksey Ch., The EU General Data Protection Regulation (GDPR), A Commentary, Oxford University Press, 2020, 315.
[110] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, 2013, 39, <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf>, [18.08.2023].

Therefore, the data processor should carefully consider the purpose or purposes for which the data will be used and should not process it if it is not necessary, adequate, or relevant for the intended purpose or purposes.[111]

It should be taken into account that defining overly broad goals jeopardizes the observance of the principle of purpose limitation. General descriptions such as "improving user experience," "marketing," "research," or "IT security" are not specific enough.[112] For example, the European Data Protection Board (EDPB)[113] explained that during video surveillance, monitoring purposes must be specified for all surveillance cameras used, and stating video surveillance is for "security" or "your safety" is not specific enough. Although a goal should not be too broad, there is no limit to how specific it can be; the exact level of Accuracy is not objectively determined by the GDPR. In many cases, it is possible to divide broad goals into multiple, more specific objectives.[114]

2.2.2. Explicitness

Explicit purposes means they must be clearly identified, explained, or expressed in a way that allows any person to have an unambiguous understanding of the processing purposes, regardless of cultural or linguistic differences.[115] There can be instances of severe violations, such as when the data controller inadequately specifies the purposes of processing, either lacking sufficient detail or clarity, or when the stated purposes are misleading or do not align with reality. In such situations, all relevant facts must be considered to determine the true purposes, along with the common understanding and reasonable expectations of the data subjects based on the context of the case.[116] The ultimate goal of this requirement is to clarify objectives without any ambiguity. The objectives must be formulated in a manner that is understandable not only to the data controller and data processors, but also to data protection authorities and interested data subjects. Particular attention should be paid to ensuring that

[111] Ibid., 15.
[112] GDPRhub, GDPR commentary, <https://gdprhub.eu/index.php?title=Article_5_GDPR#Lawful>, [18.08.2023].
[113] EDPB, Guidelines 3/2019 on processing of personal data through video devices, Version 2.0, 2020, §15, <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf>, [18.08.2023].
[114] GDPRhub, GDPR commentary, <https://gdprhub.eu/index.php?title=Article_5_GDPR#Lawful>, [18.08.2023].
[115] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, 2013, 39, <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf>, [18.08.2023].
[116] Ibid.

the specification of the objective is clear enough for all stakeholders, regardless of their different cultural or linguistic backgrounds, levels of understanding, and special needs.[117]

2.2.3. Legitimacy

Personal data must be collected for legitimate purposes. For the purposes to be legitimate, their processing at all stages and times must be based on at least one legal basis.[118] Legitimacy is a broad requirement, and it is not sufficient to merely refer to one aspect of personal data protection legislation.[119] It encompasses all forms of written and common law, including primary and secondary legislation, municipal ordinances, judicial precedents, constitutional principles, fundamental rights, general legal principles, and others.[120] It also applies to other areas of law and must be interpreted in the context of personal data processing.[121]

Customary rules, codes of conduct, codes of ethics, contractual agreements, and the general context and facts of the case can be considered when determining the legitimacy of a specific purpose. This includes the nature of the relationship between the data processor and the data subjects, whether commercial or otherwise. The legitimacy of a given purpose can also evolve over time, influenced by scientific and technological developments, as well as changes in societal and cultural attitudes.[122]

2.2.4. A New Purpose

The principle of purpose limitation aims to prevent data controllers from engaging in "secondary use" or subsequent processing of personal data when such processing is incompatible with the original purposes.[123] Any new purpose of processing that is incompatible with the original purpose must have a legal basis. Lawful processing is restricted to the original purpose, and any new purpose necessitates a separate legal basis.[124]

---

[117] Ibid., 17.
[118] Ibid.,19.
[119] Ibid., 39.
[120] Ibid., 20.
[121] Ibid., 39.
[122] Ibid., 20.
[123] GDPRhub, GDPR commentary, <https://gdprhub.eu/index.php?title=Article_5_GDPR#Lawful>, [18.08.2023].
[124] Handbook on European Data Protection Law, 2018, 140, <https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_ka.pdf>, [07.08.2023].

For instance, the use of data acquired by the data controller to verify the age of a minor is not permitted for another purpose.[125]

According to the GDPR, the use of personal data for statistical purposes, public interest, scientific, or historical research purposes will be considered compatible with the original purpose if the processing is conducted within the boundaries defined by the legislation of the European Union or a member state. However, if the secondary or further processing of the data is unrelated to the stated purposes, the data controllers must evaluate whether the further processing aligns with the original purposes.[126] To assess whether the secondary use of the data is compatible with the original purposes, the data controller must take into account:

- Any connection between the original purpose of data collection and the purpose of further processing;
- The reason on which the personal data was collected;
- Content/nature of personal data;
- The likely consequences of further data processing for data subjects;
- Existence of proper security guarantees;[127]

If the processing is deemed compatible with the original purpose, and if the above conditions are met, the presence of another legal basis is no longer necessary. However, when the processing is not compatible with the original purpose, a separate legal basis will be required (for example, the consent of the data subject before processing the data for a new purpose).[128]

2.2.5. International Judicial Practice

"In the "Schecke"[129] case, the European Court of Justice determined that the legal obligation to process personal data must adhere to the principle of proportionality, which is integral to the requirement of a legitimate purpose.[130] The court deliberated on the principle of proportionality in various cases, with one notable example being the "Digital Rights Ireland"[131]

[125] Data Protection Commission, Irish DPA, Children Front And Centre, Fundamentals for a Child-Oriented Approach to Data Processing, 2021, 48, <https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf> [07.08.2023].
[126] Eduardo Ustaran, CIPP/E, Partner, Hogan Lovells, European Data Protection Law and Practice, Second Edition, 2019, 131.
[127] GDPR, Article 6(4).
[128] Ibid., 132.
[129] CJEU, Joined Cases C- 92/ 09 and 93/ 09, Schecke [2010].
[130] The case revolved around the disclosure of personal data regarding the recipients of EU agricultural funds.
[131] CJEU, Joined Cases C- 293/ 12 and C- 594/ 12, Digital Rights Ireland [2014].

case, where the court determined the insecurity of the aforementioned principle. In this instance, the court underscored the importance of having appropriate criteria for defining relevant data and establishing data retention periods in relation to the purposes of processing.[132]

In the case of *"Digi Távközlési és Szolgáltató Kft. v. Nemzeti Adatvédelmi és Információszabadság Hatóság",* the European Court of Justice clarified the principle of purpose limitation outlined in Article 5, Paragraph 1, Subparagraph "b" of the GDPR. This provision does not preclude the registration and storage of personal data in a database created by the data controller for testing and error correction purposes, even if such data has been previously collected and stored in another database, as long as such processing remains compatible with the original purposes. Circumstances must be assessed in line with the criteria specified in paragraph 4 of Article 6 of the GDPR.[133]

2.2.6. Practice of the Personal Data Protection Service

A person's right to freely use hygienic spaces without being observed by others is a crucial guarantee of the inviolability of their personal life. Monitoring the data subject in such spaces is unjustified for any purpose. When it comes to processing minors' data, special attention should be paid to their best interests, as even accidental disclosure of such information can cause significant harm to them. Therefore, considering the large number of children in schools and the risks associated with processing private information, the Personal Data Protection Service conducted its own investigation into potential instances of video surveillance in areas designated for hygiene by various public and private schools.

As part of the inspections conducted by the Service, it was found that schools are implementing video surveillance to safeguard the safety of minors. During inspections of public schools, it was revealed that the security protection agency responsible for schools is also represented by the LEPL - Office of Resource Officers of Educational Institutions that collaborates with the school in conducting video surveillance. Several instances were identified where the area designated for hygiene (restrooms) was within the field of view of video surveillance cameras situated in the school. In some cases, it was determined that when the entrance door to the restroom was left open, the restroom area itself was visible to the video surveillance cameras

[132] Kuner Ch., Bygrave L. A., Docksey Ch., The EU General Data Protection Regulation (GDPR), A Commentary, Oxford University Press, 2020, 313.
[133] CJEU, Case C-77/21, Digi Távközlési és Szolgáltató Kft. v. Nemzeti Adatvédelmi és Információszabadság Hatóság [2022], §63.

located in the corridor. While hygiene spaces typically have doors that close, minors may be less aware of the risks of compromising their privacy and may inadvertently leave the entrance door open while using these facilities, thus exposing their actions to video surveillance cameras. As part of the inspections, violations of the law were also uncovered, and in some instances, considering the best interests of the child and to prevent breaches of minors' data, schools were issued mandatory tasks to address these issues.

2.3. Data Minimisation

2.3.1. The Essence of the Principle

According to the principle of data minimisation, data should be processed only to the extent necessary to achieve the relevant legitimate purpose. The data must be proportional to the purpose for which the processing is carried out.[134] According to the GDPR, to comply with the principle of data minimisation, the amount of processed data must be:

- *Adequate*: Sufficient to properly achieve the stated purpose.[135] Personal data is considered "adequate" if its use for a specific purpose is appropriate. For example, a person's residential address is not necessary information for assessing their creditworthiness;[136]
- *Relevant*: Having a reasonable connection to the intended purpose.[137] Personal data is "relevant" if it leads to a different result in relation to the purpose. For example, a customer's address is relevant information for the delivery of a product;[138]

[134] Law of Georgia "On Personal Data Protection", date of adoption: 14/06/2023, Subparagraph "g" of the first paragraph of Article 4.

[135] ICO, For organisations/UK GDPR guidance and resources/Data protection principles/A guide to the data protection principles/Principle (c): Data minimisation, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/> [18.08.2023].
[136] GDPRhub, GDPR commentary, <https://gdprhub.eu/index.php?title=Article_5_GDPR#Lawful>, [18.08.2023].
[137] ICO, For organisations/UK GDPR guidance and resources/Data protection principles/A guide to the data protection principles/Principle (c): Data minimisation, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/>, [18.08.2023].
[138] GDPRhub, GDPR commentary, <https://gdprhub.eu/index.php?title=Article_5_GDPR#Lawful>, [18.08.2023].

- *Limited only to what is necessary:* Not processing more data than is required to achieve the purpose.[139] This means that the purpose cannot be reasonably achieved without processing specific personal data.[140] The criterion of necessity also mandates that the retention period of personal data be limited to a strict minimum.[141]

Personal data should be processed only when the purpose of processing cannot reasonably be achieved by other means.[142] Additionally, the principle of data minimisation is closely related to the principle of purpose limitation, and it can be upheld only when specific purposes are clearly defined by the data controller. The data controller must review each step of the processing operation and each element of the data to determine its necessity in achieving the purpose.[143]

Data controllers must determine whether they need to process personal data to achieve the relevant purposes. They must verify whether the purposes can be achieved by processing a smaller amount of personal data, using less detailed or aggregated personal data, or without processing personal data at all. This assessment must be conducted before any processing begins, but it can also be performed at any point in the processing cycle.[144]

Minimisation may refer to the degree of identification. If the purpose of the processing does not require that the final set of data refer to an identified or identifiable individual (for example, in the case of statistics), even though there may be a need for identification in the initial processing (such as before data aggregation), the data controller must erasure or anonymize the personal data once the need for identification no longer exists. Additionally, if

---

[139] ICO, for organisations/UK GDPR guidance and resources/Data protection principles/A guide to the data protection principles/ Principle (c): Data minimisation, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/>, [18.08.2023].
[140] GDPRhub, GDPR commentary, <https://gdprhub.eu/index.php?title=Article_5_GDPR#Lawful>, [18.08.2023].
[141] Kuner Ch., Bygrave L. A., Docksey Ch., The EU General Data Protection Regulation (GDPR), A Commentary, Oxford University Press, 2020, 313.
[142] Handbook on European data protection law, 2018, 143, https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_ka.pdf, [18.08.2023].
[143] GDPRhub, GDPR commentary, <https://gdprhub.eu/index.php?title=Article_5_GDPR#Lawful>, [18.08.2023].
[144] EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, 2020, §74,<https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf>, [18.08.2023].

permanent identification is required for other processing activities, personal data should be pseudonymized to reduce the risk to the rights of data subjects.[145]

2.3.2. International Judicial Practice

The European Court of Justice, in the "Tele2"[146] case, determined that legislation allowing for the general and indiscriminate storage of personal data surpasses the bounds of strict necessity and cannot be deemed justified.[147]

In the case of "*TK v Asociația de Proprietari bloc M5A-ScaraA*",[148] the European Court of Justice clarified how to assess whether certain processing, such as a video surveillance system, is considered "necessary" for the purposes of protecting the legitimate interests of the data controller. The court determined that the necessity of the processing operation should be examined in conjunction with the principle of data minimisation. This principle dictates that the data controller should only pursue adequate, relevant, and non-excessive purposes for processing.[149]

2.3.3. Practice of the Personal Data Protection Service

- *The teacher of one of the public school*

[145] Ibid., §75.
[146] CJEU, Joined Cases C- 203/ 15 and C- 698/ 15, Tele2 [2016].
[147] Kuner Ch., Bygrave L. A., Docksey Ch., The EU General Data Protection Regulation (GDPR), A Commentary, Oxford University Press, 2020, 313.
[148] CJEU, Case C-708/18, TK v Asociația de Proprietari bloc M5A-ScaraA, [2019].
[149] GDPRhub, GDPR commentary, <https://gdprhub.eu/index.php?title=Article_5_GDPR#Lawful>, [18.08.2023].

Based on the notification from the Internal Audit Department of the Ministry of Education and Science of Georgia, the Personal Data Protection Service investigated the lawfulness of a school teacher disclosing children's data in Messenger groups.

During the inspection, it was discovered that during a lesson, a tutor's remarks about disabled people triggered a strong reaction from one of the students, who had a sibling with a disability attending the same school. The parent of the minor intervened to address the incident and informed the school director.The parents of other students in the class also showed interest in the incident and discussed the case during a meeting. Subsequently, the mother of the minor involved addressed the school's disciplinary committee. The proceedings concluded with a reprimand for the tutor. However, prior to the committee's decision, the tutor posted photos of his written response to the parent's statement in two separate Messenger groups.

Within the study, attention was focused on the purpose of creating the specified groups. It was determined that up to 30 parents of the students in the class joined one of the groups for the immediate exchange of information between the teacher and parents regarding organizational issues and the educational process. The second group consisted of more than 30 school employees and was created for communication between the school administration and teachers during distance learning. The material disclosed by the teacher in the groups included excerpts from the text of the student's parent's statement, the teacher's comments on them, as well as the content of conversations, opinions expressed during and after the lesson, identification data of minors and individuals related to them, confidential circumstances investigated and evaluated as part of the ongoing disciplinary proceedings related to the incident. Additionally, the material included the name and surname of another student, the content of communication with them, and students' attitudes towards specific facts. The teacher clarified that they disclosed the mentioned information to safeguard their own truth and reputation, perceiving the unfolding events as detrimental to his teaching endeavors.

In assessing the matter, the Service underscored that data acquired within the scope of pedagogical activities should be processed with paramount consideration for the best interests of children. Moreover, emphasis was placed on the pivotal role of caregivers (including teachers) in safeguarding the personal and familial lives, dignity, well-being, free personality development, safety, and other rights of minors. It was clarified that every data controller may possess a legitimate interest in safeguarding their professional reputation, particularly when disciplinary proceedings are underway concerning their official actions and the professional community is apprised of the situation. Nonetheless, even with a legitimate interest present, it's imperative to exercise extreme caution regarding the volume of data and to discern which

information is necessary for achieving the legitimate goal while minimizing interference with the minor's right to privacy. In evaluating the lawfulness of data disclosure, they also referenced the definition provided by the European Court of Justice (referenced in the case: Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González [GC], C-131/12, 13 May 2014), which underscores the fundamental importance of not publishing data beyond the scope of necessity (e.g., for public information). It was determined that the teacher could safeguard his professional reputation by processing less data, merely stating their general position in Messenger groups, without disclosing personal data or delving into excessive detail regarding the circumstances.

As per the decision of the Service, the teacher was found to have violated the principle of minimisation of personal data processing, resulting in an administrative fine being imposed. Additionally, was instructed to promptly erasure the unlawfully disclosed address and photos. The teacher complied with these directives within the shortest possible timeframe following the issuance of the decision.

- *One of the Private Hospital*

The health-related data include particularly sensitive information about a person's private life, mental and physical condition. The unlawful acquisition, disclosure or other data processing of a similar nature about an individual may not only be a violation of privacy but also the cause of indignity, stigmatization or discrimination. Thus, the confidentiality of health related data necessitates special protection. This is why international and Georgian Law sets high standards and safeguards for the protection of health-related data. On the basis of a citizen's application, the Personal Data Protection Service of Georgia examined the lawfulness of the information disclosed by the director of the hospital in a telephone comment to a television company, which concerned the health condition of the applicant's deceased son (including the congenital disease, treatment procedures performed, etc.). According to the applicant, his deceased minor son had overcome the health problems listed and disclosed by the hospital director and had been fully rehabilitated a year and a half before the telephone comment. Thus, the surgeries and other congenital health problems listed by the doctor had no relation with the health condition and death of the applicant's son.

According to the information provided by the hospital in the process of examining the lawfulness of data processing, the provision of information in telephone commentary served to protect the interests of the hospital, because the child's parents and family members had disseminated the inaccurate information via the media. The patient had many comorbidities from birth which, all together, further resulted in the minor's death. Thus, the purpose of the

disclosure of the information referred to in the Medical Director's telephone commentary on behalf of the hospital was to protect the reputation of the hospital and to provide the public with accurate information on the matter. Within considering the application, the Service stated, that the hospital had no need to disclose that extent of the data, as it was done in the telephone comment by the Medical Director of the hospital. As part of the inspection, the hospital was able neither to justify the need for disclosure of detailed information, nor the reason why only the general reference to the child's health status would not suffice to achieve the objective of the hospital. Occasioned by this, the data publicized by the hospital director was not considered as adequate and proportionate. By the decision of the President of the Personal Data Protection Service of Georgia, the hospital was held administratively liable for the administrative offence under Article 44, paragraph 1 of the Law of Georgia "On Personal Data Protection" (Violation of principles of data processing).

2.4. Authenticity and Accuracy

2.4.1. The Essence of the Principle

The principle of data accuracy stipulates that data must be authentic, precise, and, where necessary, kept up to date. In accordance with the purposes of data processing, any inaccurate data should be rectified, erased, or destroyed promptly.[150] While the GDPR does not explicitly define "accuracy", in practice, "inaccurate" data is understood to encompass any information that is incorrect or misleading. This includes objective facts pertaining to an individual, such as their name, date of birth, or residential address, thus falling within the purview of Article 5, paragraph 1, subparagraph "d" of the Regulation. In addition, the principle of accuracy applies not only to facts about a person, but also to predictions and assumptions, which is particularly pertinent for contemporary methods of automatic profiling, data processing through artificial intelligence, or other modern systems. Predictions may be deemed objectively inaccurate if they rely on erroneous facts, flawed reasoning, or methodologies. Consequently, both data controllers and processors must adhere to the principle of accuracy, ensuring that data processing is based on reliable information. Unlike evidence-based predictions and assumptions, value judgments cannot be considered "inaccurate" as they are inherently subjective.[151] In practice, the principle of data accuracy entails:

[150] Law of Georgia "On Personal Data Protection", date of adoption: 14/06/2023, Subparagraph "d" of the first paragraph of Article 4.
[151] GDPRhub, GDPR commentary, <https://gdprhub.eu/index.php?title=Article_5_GDPR#Lawful>, [18.08.2023].

- Reasonable measures should be implemented to verify and maintain the accuracy of personal data;
- The origin of personal data must be transparent and identifiable;
- Any discrepancies regarding data accuracy should be thoroughly investigated and addressed;
- The need to periodically update the information should be assessed;[152]

The requirements for data accuracy should be assessed in light of the potential risks and impacts associated with the specific use of the data. Inaccurate personal data can pose risks to the rights and freedoms of the data subject, potentially leading to decisions being made on inappropriate grounds, whether manually, automatically, or through artificial intelligence.[153] Therefore, it is the responsibility of the data controller to uphold the principle of data accuracy across all processing activities.[154]

Data accuracy holds particular significance in the context of age verification, also known as age attestation.[155] Therefore, data controllers must closely monitor and address any challenges related to data accuracy. For instance, a child who gains access to services intended for both minors and adults at an older age may unknowingly consent to data processing that leads to

[152] ICO, For organisations/UK GDPR guidance and resources/Data protection principles/A guide to the data protection principles/Accuracy, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/accuracy/>, [18.08.2023].
[153] EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, 2020, §78, <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf>, [18.08.2023].
[154] Handbook on European Data Protection Law, 2018, 145 <https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_ka.pdf>, [18.08.2023].
[155] For instance, to access movies with age restrictions, an individual may be prompted to provide their age electronically.

inappropriate profiling.[156] Hence, it's crucial for data controllers conducting age verification to consider the risks and potential harm associated with age verification bypasses.[157]

2.4.2. Foreign Practice

In a case concerning a data subject's request for the right to rectify data, the Federal Administrative Court of Germany[158] ruled that the data controller cannot be compelled to amend and process data whose accuracy cannot be sufficiently determined.[159] In such instances, processing such data would contravene the person will violate the Subparagraph "d" of the first paragraph of Article 5 of the "GDPR" and the second paragraph of the same article. Therefore, the burden of proof regarding the accuracy of the data to be updated falls on the data subject. In the specific case mentioned, as the data subject could not confirm their date of birth, the court ruled in favor of the data controller.[160]

2.4.3. Practice of the Personal Data Protection Service

- *Inspection of the LEPL - Education Management Information System*

The Personal Data Protection Service, on its own initiative, studied the lawfulness of the processing of personal data of the students of the LEPL - Tbilisi Classical Gymnasium by the

[156] According to the GDPR, profiling refers to the processing of personal data in any automated form, involving the use of personal data to evaluate certain personal characteristics related to an individual. Profiling is an area where the personal data of minors receives special protection. It can serve various purposes, including offering or delivering content to users in the online context. Additionally, it may be utilized to ascertain or estimate a user's age for child protection or crime prevention purposes. Profiles typically rely on a user's previous online activities or browsing history. See: General Data Protection Regulation, GDPR, Article 4 (4), Recital 38; ICO, Age appropriate design: a code of practice for online services, Profiling, <https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/12-profiling/>, [18.08.2023].

[157] ICO, Information Commissioner's opinion: Age Assurance for the Children's Code, 2021, 26-27, <https://ico.org.uk/media/4018659/age-assurance-opinion-202110.pdf>, [18.08.2023].

[158] BVerwG (Germany), 6 C 7.20, [2022], <https://gdprhub.eu/index.php?title=BVerwG_-_6_C_7.20>, [18.08.2023].

[159] GDPR, Art. 16.

[160] GDPRhub, GDPR Decision Database, <https://gdprhub.eu/index.php?title=BVerwG_-_6_C_7.20>, [18.08.2023].

General Education Management Information System of the LEPL - Education Management Information System.

It's important to note that the general education management information system (referred to as eSchool) contains a substantial amount of personal data for each student attending public and private general educational institutions across Georgia. This data includes special category information such as name, surname, personal identification number, date of birth, citizenship, address, class, and details regarding the student's status, such as whether they have disabilities, are socially vulnerable, displaced, a refugee, humanitarian, asylum seeker, among others. Additionally, the law mandates various electronic processes within the eSchool, involving the collaboration of general educational institutions and technical support from the LEPL - Education Management Information System (referred to as the information system). These processes include student enrollment, expulsion, suspension and restoration of status, class advancement, mobility, and timetable creation. It's worth noting that the LEPL - - Tbilisi Classical Gymnasium (referred to as the Gymnasium) is one of the most populous among the general educational institutions operating within the Tbilisi Municipality. At the time of inspection, the Gymnasium had 2181 students enrolled.

During the inspection, it was discovered that the information system within the eSchool, in contravention of Article 4, Subparagraph "g" of the law, processed students' photos in a manner disproportionate to the lawful purpose of data processing, lacking proper necessity and legitimate purpose. These photos were transferred to the information system from the database of the LEPL - Public Service Development Agency. It is notable that according to "Regarding the Approval of Rules and Conditions for the Creation and Administration of the General Education Management Information System" Order No. 08/N of the Minister of Education, Science, Culture and Sport of Georgia dated February 9, 2021, paragraph 4 of Article 2 exhaustively delineates the list of data stored in the electronic database of the LEPL - Public Service Development Agency. This data, pertaining to natural persons and reflected in the eSchool for purposes of identification/verification and/or determination/verification of their citizenship status, may be received and processed by the information system. However, it's important to highlight that a photograph is not included in the aforementioned list.

During the inspection, it was discovered that within the eSchool, information regarding the statuses of socially vulnerable persons, forcibly displaced persons, and persons with disabilities was managed in the following manner: when a parent submitted an application for enrolling a minor in the gymnasium, they were informed that they could voluntarily provide information in the eSchool regarding these statuses. Subsequently, upon submission of relevant

supporting documents, the gymnasium would record the corresponding status(es) of the minor in the eSchool. Furthermore, parents were only informed about the submission of this data at the time of the initial application, with no follow-up communication to ascertain whether these statuses had changed over time.

It's noteworthy that the data entry process in the eSchool system regarding the statuses of socially vulnerable persons, forcibly displaced persons, and persons with disabilities was based solely on voluntary submission of documents by parents confirming these statuses. Consequently, there's a notable possibility that some high school students who may actually have these statuses might not have them reflected in their eSchool profiles if their parents didn't submit the required documents. Moreover, once these statuses were marked for high school students, there wasn't a mechanism in place to update or verify whether these statuses changed over time. Consequently, there's a risk that students who were marked with these statuses in the eSchool system may no longer meet the criteria for such statuses, yet their data remained unchanged. Indeed, the method employed to record and store information regarding the statuses of socially vulnerable persons, forcibly displaced persons, and persons with disabilities among high school students fails to ensure the processing of accurate and updated data, as mandated by Article 4, Subparagraph "d" of the Law of Georgia "On Personal Data Protection".

It appears that eSchool records the results of a survey regarding high school students' access to computer devices and the Internet. While the information system explained that this processing serves the planning and implementation of appropriate measures in the event of the need to switch to distance learning, it was not clarified why the old survey results, pertaining to previous years, regarding the possibility of distance learning are stored for each student.

During the inspection, it was found that after students' active status was terminated, their data was not fully archived in eSchool, meaning access to this data by those with eSchool access was not restricted. The information system plans to activate this functionality by February 2026. Before this period, it was also planned to issue the individual administrative-legal act of the head of the information system, which determined the persons with the authority to access the archived data. It is noteworthy that data archiving aims to minimize access to data by different individuals, particularly to restrict the access of employees from various institutions with access to eSchool to data that may not be necessary for them to fulfill their designated duties. Therefore, the Personal Data Protection Service has deemed it appropriate for the information system to promptly assess, within a defined timeframe, the necessity of access by

employees of various entities within the system to the data of students with inactive status processed in the eSchool. Access to this data should be restricted to employees who do not require it.

As part of the inspection, it was also determined that the database utilized for the operation of the eSchool system, through direct access from the database management system, did not record successful data browsing during the data processing process. This lack of recording does not comply with the requirements outlined in Article 17 of the Law.

During the on-site inspection at the gymnasium, it was observed that gymnasium administrators and information managers were utilizing shared user accounts in eSchool. The evidence presented in the case materials did not confirm that the gymnasium had requested the information system to create personalized accounts for all case managers and information managers in eSchool. This constitutes a violation of the requirements outlined in Article 17 of the law.

As a result of the inspection, the information system was found to have violated administrative offenses outlined in Article 44 and Article 46 of the Georgian Law "On Personal Data Protection" due to breaches in data processing principles and failure to comply with data security protection requirements. Similarly, the gymnasium was found to have violated the same law by failing to adhere to data security protection requirements, constituting an administrative offense as per Article 46. Additionally, the information system was directed to: halt the processing of students' photographs in eSchool; Implementing organizational and technical measures for data security that guarantee the logging of all actions carried out on the data within the eSchool database (during direct database access); Evaluating the necessity of access to data of students without an active status processed in eSchool by employees of various institutions and limiting access to this data for those employees who do not require such access. Assessing the necessity of retaining past (prior-year) survey results pertaining to students' potential engagement in remote learning within the eSchool, as well as considering the handling of information regarding students no longer active, including the options of erasure, destruction, or storage in a manner that ensures non-identifiability following the expiration of the required retention period. The information system and the gymnasium were directed to adhere fully to the stipulations outlined in Article 4, Subparagraph "d" of the Law of Georgia "On Personal Data Protection", ensuring the processing of information concerning the statuses of gymnasium students as socially vulnerable individuals, persons with disabilities, and forcibly displaced persons in a manner that guarantees the accuracy and integrity of such data.

2.5. The Storage Limitation

2.5.1. The Essence of the Principle

The principle of storage limitation means that data can only be kept for the duration necessary to fulfill the legitimate purpose of data processing.[161] The data controller must inform the data subject in advance about the storage period and ensure adherence to this principle. Consequently, the retention period should be established within the organization before data processing commences.[162]

In the process of processing personal data, storage period limitation is crucial because storing data for an excessive period renders it unnecessary, thereby eliminating the legal basis for its processing. Practically speaking, retaining personal data longer than necessary leads to increased storage and security costs. Furthermore, the longer data is stored, the higher the likelihood of data subjects requesting access to or erasure of their information.[163]

---

[161] See, Law of Georgia "On Personal Data Protection", date of adoption: 14/06/2023, Subparagraph "e" of the first paragraph of Article 4. According to Subparagraph "e" of the paragraph 1 of Article 5 of the "GDPR" and Subparagraph "e" of the paragraph 4 of Article 5 of the modernized version of Convention 108 of the Council of Europe, personal data must be stored in a form that allows the identification of data subjects for no longer than necessary for the purposes of data processing.

[162] GDPRhub, GDPR commentary, <https://gdprhub.eu/index.php?title=Article_5_GDPR#Lawful>, [18.08.2023].

[163] ICO, For organisations/UK GDPR guidance and resources/Data protection principles/A guide to the data protection principles/The principles/Storage limitation, <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/the-principles/storage-limitation/#why_storage_limitation>, [18.08.2023].

Personal data storage periods can be accurately determined by considering the following factors:

- The Data Controller must consider the stated purpose(s) for data collection. Data may be retained as long as it is necessary to achieve at least one of the purposes. However, storage of data is not justified in "just in case" basis, or if there is only a very small chance that the data will be useful;
- The data controller must determine whether records of the legal relationship (for example, the provision of services to minors) need to be kept after the legal relationship has ended. It may be unjustified to delete all data immediately after the end of the legal relationship; retaining some information or small details may be necessary to confirm the existence or termination of the legal relationship;
- The data controller must consider whether the information needs to be stored to protect potential legal interests. Information that is not relevant to protecting these legal interests can be deleted. If there is no other reason for retaining the data, personal data must be erasure once the need for such legal protection can no longer arise;
- The data controller must consider the legal requirements related to data storage. Regulations and guidelines exist for retaining certain categories of data, such as information for educational, tax, audit, health, and safety purposes. If the data controller stores information based on these requirements, it is less likely that the data will be retained for an excessive period of time;
- The data controller must take into account the standards and instructions relevant to their field of activity. However, the mere existence of such standards does not, in itself, confirm compliance with the principle of storage period limitation. The data controller will need to justify the necessity and appropriateness of these standards;
- When determining the time limits, the Data Controller should adopt a proportional approach to balance their needs with the impact of the storage periods on the child's personal life and best interests. Additionally, it should be ensured that the storage periods should always be fair and legal;[164]

2.5.2. General Court Practice

In the case of "*Aycaguer v. France*," the European Court of Human Rights noted that, at the time, the country lacked provisions for determining storage terms based on the nature and severity of the crime committed. The regulations regarding the storage of DNA profiles in the

[164] Ibid.

database did not provide adequate protection to data subjects, considering both the length of time the data was stored and the inability to erase the data. Consequently, the European Court concluded that the regulations in force could not ensure a fair balance between conflicting public and private interests.[165]

In the case "*Digi Távközlési és Szolgáltató Kft. v. Nemzeti Adatvédelmi és Informationációszabadság Hatóság*," the European Court of Justice elucidated the principle of storage limitation outlined in Article 5, Paragraph 1, Subparagraph "e" of the GDPR. Specifically, the principle mentioned precludes the reutilization of data previously gathered for a different purpose by the data controller and the processing of such data in a database established for error correction beyond the duration necessary for testing and rectifying errors.[166]

2.5.3. Practice of the Personal Data Protection Service

- *Inspection of LEPL - Agency for State Care and Assistance for the Victims of Human Trafficking*

The Child Rehabilitation/Habilitation Sub-program is one of the sub-programs designated for implementation based on Resolution No. 69 of the Government of Georgia, dated February 21, 2023, "On the Approval of the 2023 State Program for Social Rehabilitation and Child Care." Within this sub-program, aimed at bolstering children with disabilities and their families, actualizing the physical and intellectual functional potential of the children, enhancing overall health and quality of life, and fostering inclusive development, an individual rehabilitation/habilitation plan is devised and executed for each beneficiary by a team of relevant specialists. This process includes the implementation of therapeutic interventions and various other types of therapies. Based on the application submitted by the legal representative of the minor for enrollment in the sub-program, the trafficking agency processes a substantial amount of personal data concerning disabled minors (for example, this includes information on health status, disability status, reintegration allowance, socially vulnerable person status, rating scores, etc.) The inspection involved examining the lawfulness of processing personal data via electronic systems for reviewing applications submitted by the Trafficking Agency to the Tbilisi City Center for inclusion in the aforementioned sub-program.

[165] Case of Aycaguer v. France, [2017] ECHR App. No. 8806/12, §§42-43, 45, 47.
[166] CJEU, Case C-77/21, Digi Távközlési és Szolgáltató Kft. v. Nemzeti Adatvédelmi és Információszabadság Hatóság [2022], §63.

During the inspection, it was uncovered that data processing for the implementation of the Child Rehabilitation/Habilitation Sub-program occurs through the trafficking agency's electronic proceedings program and a dedicated web portal. Moreover, in administering these systems, the trafficking agency engages the services of an authorized entity, namely the LEPL - Information Technology Agency. Among its responsibilities, this agency provides technical support for the systems and manages customer relations in alignment with the agency's objectives.

Within the rehabilitation/habilitation module of the web portal, among other categories of data, there are plans to input details regarding the employment status of the legal representative of the sub-program beneficiary, as well as information regarding any additional sources of funding for the beneficiary. However, during the inspection it was found that this data is deemed unnecessary and is not utilized in the implementation of the rehabilitation/habilitation sub-program. Despite the absence of the mentioned information in the portal during the inspection, the Service clarified that the presence of relevant fields posed a risk of registrants filling them incorrectly for different applicants. This could lead to an unnecessary amount of data processing not aligned with the purpose and requirements of the sub-program implementation. Consequently, the Service deemed it appropriate to remove the "Employment" and "Other types of financing" fields from the rehabilitation/habilitation module of the web portal.

During the inspection, it was also discovered that data in the rehabilitation/habilitation module of the web portal is stored indefinitely, despite the trafficking agency not having assessed the storage period based on the necessity of retention. Therefore, to uphold the principle of data processing outlined in Article 4, subparagraph "e" of the Law of Georgia "On Personal Data Protection," the Trafficking Agency was directed to establish the specified timeframes in proportion to the intended purpose of data processing, while considering the necessity for data retention and legal requirements.

In several instances, the trafficking agency failed to fulfill its obligation to implement the requisite organizational and technical measures to safeguard security during the processing of data via the web portal and the electronic case management program. Specifically:

- Concerning the 143 individuals with active accounts in the web portal, the trafficking agency failed to specify their identities and the authority under which they required access to the information processed within the sub-program framework. Notably, access to the web portal by these individuals was feasible from the open Internet

network, granting them the ability to reset passwords as needed. Additionally, former agency employees retained access to the aforementioned portal;

- Some of the agency's employees with access to the rehabilitation/habilitation module in the web portal did not require access to the entirety of the information processed within the module to carry out their designated functions within the scope of their duties;
- In instances of direct access to the electronic case management program and the web portal database servers, incomplete recording of information regarding data processing in the web portal was observed. Furthermore, employees authorized to access the said database utilized a shared user account;
- The electronic case management program did not predefine the complexity or required number of characters for passwords, allowing for the use of any password, including simple ones;
- For the purpose of deciding on the inclusion of applicants in the sub-program, as well as providing reasons for refusal to include them, unified lists of applicants were distributed to each territorial unit of the Agency through the electronic case management program. Consequently, these lists became accessible to agency personnel, even those who did not require access to the complete information contained within them;
- The official accounts established for service-providing medical institutions on the web portal were not customized for the respective employees of those organizations. The identities of the employees utilizing the accounts created for these organizations were unknown to both the Trafficking Agency and the LEPL - Information Technology Agency;

During the inspection, it was uncovered that the Trafficking Agency provided information about the dismissal of several employees to the LEPL - Information Technology Agency. In two of these cases, the employees were explicitly instructed to deactivate the personalized users from the web portal. However, the authorized person failed to ensure the fulfillment of these requests, leading to the continued activity of the mentioned users at the time of the inspection.

Based on the information provided, the Trafficking Agency was held responsible for committing an administrative offense under Article 46 of the Law of Georgia "On Personal Data Protection." Additionally, the LEPL - Information Technology Agency was deemed responsible for an offense under the first paragraph of Article 52 of the same law. In order to

ensure data security in the future, the Trafficking Agency and the LEPL - Information Technology Agency were instructed to: Record all the actions performed on the data in the rehabilitation/habilitation module of the web portal, as well as in the databases of the web portal and the electronic case management program (during direct access to the database). Adopt such organizational and technical measures, as a result of which the authorized persons will access the mentioned databases only with the personalized accounts of the users protected by the appropriate password. Access to the data processed within the framework of the sub-program via the rehabilitation/habilitation module of the web portal is exclusively granted to individuals who require such data to fulfill their designated functions and responsibilities. Each employee necessitating access to the same module is granted access solely to the information essential for executing the duties assigned to them by law. Furthermore, employees are permitted access to the electronic case management program solely through the utilization of a complex password of appropriate complexity. The Trafficking Agency received additional instructions to send only the lists of applicants to each of its territorial units via the electronic case management program for the purpose of determining whether to include them in the sub-program or providing explanations for refusal. Each territorial unit is required to render a decision or provide an explanation for refusal regarding the applicants assigned to them.

2.6. Data Security

2.6.1. The Essence of the Principle

During data processing, it's essential to implement technical and organizational measures that sufficiently guarantee data protection, including protection against unauthorized or unlawful processing, accidental loss, destruction, or damage.[167] The security of personal data requires appropriate measures to prevent and manage incidents, ensure the proper performance of data processing tasks and compliance with other principles, and promote the effective implementation of individuals' rights.[168] Security measures should encompass not only cyber security but also physical and organizational security. It's crucial for organizations to conduct

[167] See, Law of Georgia "On Personal Data Protection", date of adoption: 14/06/2023, subparagraph "v" of paragraph 1 of article 4.

[168] EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, 2020, §83, <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf>, [18.08.2023].

regular assessments to ensure that their security measures remain up-to-date and effective.[169] When adopting appropriate data security measures, organizations should consider modern data security methods and technologies,[170] recent advancements, implementation costs, as well as the nature, scope, context, and goals of processing. Additionally, the impact of processing operations on the rights and freedoms of individuals should be taken into account.[171]

2.6.2. General Court Practice

The European Court of Human Rights has rendered several decisions regarding data security matters. In the case of "*Z v Finland*,"[172] the European Court ruled that domestic legislation should include adequate security measures to prevent any communication that contradicts the safeguards outlined in Article 8 of the "European Convention on Human Rights" or the disclosure of health information. Specifically, Finland was found to have failed in ensuring the implementation of adequate technical and organizational measures to safeguard against unauthorized access to patient medical data within a public hospital.[173]

2.6.3. Practice of the Personal Data Protection Service

- *Inspection of small family type houses*

One of the sub-programs designated for implementation within the framework of the childcare program, as approved by the decree of the Government of Georgia, is specialized family-type services for children with severe and profound disabilities or health issues. The aim of this service provision, as outlined in the resolution, is to offer care and education in

[169] Irish DPA, Quick Guide to the Principles of Data Protection, 2019, <https://www.dataprotection.ie/sites/default/files/uploads/2019-11/Guidance%20on%20the%20Principles%20of%20Data%20Protection_Oct19.pdf >, [18.08.2023].

[170] Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 10.X.2018, §63, <https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a>, [18.08.2023].

[171] GDPRhub, GDPR commentary, <https://gdprhub.eu/index.php?title=Article_32_GDPR#cite_note-1>, [18.08.2023].

[172] Case of Z v. Finland, [1997], ECHR, App. No. 22009/93.

[173] Kuner Ch., Bygrave L. A., Docksey Ch., The EU General Data Protection Regulation (GDPR), A Commentary, Oxford University Press, 2020, 634.

environments closely resembling family settings. This involves placing children with severe and profound disabilities or health issues, who lack care, in environments that closely resemble their own families. Considering the aforementioned context, given that the organization managing small family-type houses processes a significant volume of data belonging to minor disabled beneficiaries, including special categories of data, the Personal Data Protection Service initiated a review of the lawfulness of the data processing conducted by service provider organizations of the small family-type houses under their management. This initiative encompassed a total of two small family-type houses.

During the inspection, it was established that small family-type houses process documents containing the personal data of beneficiaries, including special categories of data. These data are obtained by the small family-type houses both from the LEPL - Agency for State Care and Assistance for the Victims of Human Trafficking and on the other hand, considering the needs identified directly during service provision through various means (such as educational activities, within the treatment supervised by the organization, etc.). Furthermore, within the framework of the inspection and based on information provided by the agency, organizations, and relevant legal provisions governing the organization's activities, it was determined that legislation mandates the organization to produce journals and "Personal files." These files are where copies of individual development plans, individual service plans, and information related to the beneficiary's education, health, and other matters are stored. Consequently, based on the evidence gathered during the inspections, it was established that the organization processes the personal data of beneficiaries, including special category data, to the extent necessary to achieve a specific and clearly defined legal objective.

During the inspections, it was also discovered that alongside processing data in physical form, the organization employs technical means for processing beneficiary data, including a portable computer (commonly referred to as a "laptop") and personal email addresses of individuals authorized to access the data. These tools are utilized for the exchange of information and documentation containing beneficiaries' personal data. Specifically, it was found during the inspection that the laptop computer used for processing the personal data of beneficiaries belonged to the head of a small family-type household. During both inspections, it was discovered that the laptops utilized for data processing lacked password protection, and the passwords for the email addresses were stored in the laptops' memory. This situation enables any individual with access to the computers to access the personal data of beneficiaries, including special categories, stored in the emails. Moreover, in one of the inspections, it was

further revealed that a laptop used for processing beneficiaries' personal data was shared among multiple employees of a small family-type home. However, these employees did not utilize the computer under individual (personalized) user accounts.

It's important to note that the exchange of professional information among organization employees through personal email poses significant challenges. This is because personal email systems allow employees to access data, including from other electronic devices, and the control of this access cannot be entirely reliant on the organization's organizational and technical measures. Additionally, the possibility of data access remains available to employees even after the termination of their official employment relationship with the data controller. The existing provisions regarding confidentiality of official information in the organization's bylaws, labor contracts, and a separate document regulating the protection of beneficiaries' personal data cannot be deemed as adequate organizational and technical measures to mitigate risks and ensure data security within the organization. This is particularly critical considering that the organization handles a significant amount of data on minors, including special category data. Therefore, it was concluded during the inspection that the organization had not implemented appropriate organizational and technical measures for ensuring data security.

Taking into account the above, the organizations were held responsible for the administrative offense provided for in the first paragraph of Article 46 of the Law of Georgia "On Personal Data Protection". In addition, the organization was ordered to use only an e-mail address created for official purposes in the process of processing data in electronic form, and when processing data through a laptop computer, to use an account created only for official purposes, which will be properly protected with a password and used only for official purposes. In addition, in the process of processing beneficiary data in electronic form, for each person with the right to access a laptop computer, create an individual user, which will be properly protected by a password.

- *Inspection of the City Hall of Rustavi Municipality*

Within the framework of the implementation of health care programs and sub-programs, municipalities also use automated means to process large volumes of data, including special categories of data on vulnerable groups such as minors. Ensuring compliance with data security rules for this data necessitates an adequate risk assessment. The inspection was carried out at the initiative of the Service and included the study of the lawfulness of the processing of

personal data of the beneficiaries during the implementation of the rehabilitation sub-program for children with autism spectrum disorders.

As part of the inspection, it was established that to include children with autism spectrum disorders in the rehabilitation sub-program, a significant amount of information about the beneficiary, including health information, was submitted to Rustavi City Hall along with the application. The application to the City Hall was submitted both in material form and through Rustavi City Hall's email or the citizen's electronic portal. The electronic copy of the application and the attached documentation was first loaded into the electronic case management program, where a number of data about the beneficiary and their legal representative (name, surname, personal number, date of birth, photograph, etc.) were automatically reflected from the database of the LEPL - Public Service Development Agency. For the purposes of implementing the sub-program, electronic documents in the format of "MS Excel" were also created, updated, and used, containing several personal data of the beneficiary. The operation of the electronic case management program and the citizen portal was technically ensured by MSDA Municipal Services Development Agency.

Within the scope of the inspection, it was determined that by using certain search functionalities in the electronic program of the Municipality of Rustavi, it was possible to access any correspondence within the program. Some employees with service accounts in the electronic case management program had activated functionalities and access to a large volume of data processed within the framework of the rehabilitation sub-program for children with autism spectrum disorders. However, the inspection revealed that some of these employees did not need access to the beneficiaries' data to perform their assigned functions and duties. For example, at the time of the inspection, a total of 39,277 correspondences registered in the case management program were available to these employees, including correspondences related to beneficiaries with autism.

As a result of the inspection, it was also revealed that the common shared folder, which allowed City Hall employees to access electronic documents in MS Excel format containing the personal data of the beneficiaries, did not have an electronic log for recording the actions taken on the data. This created a risk that, in the event of unlawful processing of data, including unauthorized disclosure by employees with access to the data, the relevant fact and the identification of the responsible person could not be recorded.

As part of the inspection, it was established that for the purposes of the electronic case management program and the citizen's portal, data was received from the database of the LEPL - Public Service Development Agency. However, the contract signed between the agency and Rustavi municipality did not provide for the provision of photos of individuals to Rustavi City Hall, nor did it account for the real-time provision of data to the citizen portal of Rustavi City Hall.

According to the decision of the Service, the City Hall of Rustavi municipality was held responsible for the administrative offense provided for in the first paragraph of Article 46 of the "Personal Data Protection" Law of Georgia for non-compliance with data security requirements. In addition, the City Hall was instructed to record all actions taken in relation to the data of the beneficiaries (including the data in the common shared folder), as well as to implement measures to prevent the transfer of data processed in the electronic case management software to third parties in violation of the law. Access to this data should be granted only to those persons who need it to perform their assigned functions. Rustavi City Hall and the LEPL - Public Service Development Agency were also directed to comprehensively address the matter of receiving personal data from the mentioned agency in real-time and in a volume proportional to the processing purpose during the operation of the electronic case management program and the citizen's portal, with a contractual agreement in place.

- *Inspection of one of the Public Schools*

The inspection was carried out at the initiative of the Service because schools process a significant amount of personal data about minors' disciplinary offenses, including by automatic means. The failure to implement appropriate organizational and technical measures for this data may lead to illegal disclosure or other forms of processing, which can harm the child's dignity, lead to stigmatization, and become a determining factor in "bullying" and discrimination.

As part of the inspection, it was established that the school was processing student data within the framework of disciplinary violations, including using automatic means (electronic journal). The acting school director and their deputy, in the field of registration of violations of the electronic journal, programmatically obtained data related to student disciplinary offenses from the electronic information database of the Office of Resource Officers, including information about the location, time of the violation, and the event conducted by the law

enforcement officer. In addition, the student's first name, last name, personal number, date of birth, gender, class, and social status were reflected in the violation field of the electronic journal from the education management information system ("eSchool"). During disciplinary proceedings, the school received a written explanation from the student regarding the alleged violation, and the extent of the student's responsibility was determined by the school director through an individual administrative-legal act. The electronic journal, the electronic information base of the Office of Resource Officers, and the software of "eSchool" were implemented by the Education Management Information System.

As part of the inspection, it was determined that the search and browsing actions were not recorded in the electronic log. Similarly, actions performed on the data were not recorded in the case of direct access to the database used to store the data in the electronic log. Additionally, administrators of the database of LEPL - Education Management Information System used the same users in the case of direct access to the database. It's worth noting that even when actions taken on the data are recorded, access by a common user makes it challenging to identify the individual performing a specific action, thus not meeting data security protection requirements.

According to the decision of the Service, LEPL - Education Management Information System was recognized as a violator for committing an administrative offense (failure to comply with data security requirements) provided for in Article 46 of the Law of Georgia "On Personal Data Protection". In addition, the system was instructed to record all actions performed on the data in the electronic journal, as well as in the database (during direct access to the database). Furthermore, the adoption of organizational and technical measures was mandated, whereby authorized persons would be able to access the electronic journal database only through individual user accounts protected by proper passwords.

- *Inspection of the Vake District Administration of Tbilisi Municipality*

It is worth noting, that a large volume and sensitive category of information about minors is processed by the district administrations of the municipality during recruiting the conscripts for the military registration. In line with the mentioned the risk of illegal processing is increasing. Thus, on its own initiative the Personal Data Protection Service of Georgia examined Vake District Administration of Tbilisi Municipality, which comprised the examination on the lawfulness of minors' personal data processing by the Administration for the purpose of recruitment of conscripts for military registration.

The inspection on the lawfulness of personal data processing stated that for the purpose of the initial registration of minors Vake District Administration of Tbilisi Municipality performs the manual processing of personal data of minors - through obtaining "questionnaires" filled in by students/legal representatives of students, "communication forms", copies of identity cards and birth certificates, photos, as well as via electronic system including their collection, utilization and storage. In addition, the inspection revealed that the electronic system, through which the initial registration of minors as well as data processing for the purposes of conscription for military service are carried out, is administered by the structural unit of the administration of Tbilisi City Hall - the Secret Mobilization Service. Accordingly, its data processors have access to the data in the said electronic system.

As part of the inspection, it has been stated that the procedures for primary military registration and the role, powers and documentation to be provided by each entity involved in this process (municipality, educational institution, conscript) are determined by Decree No. 247 of the Government of Georgia of 02 June 2015 "On Approval of the Regulation on Military Registration of Citizens". According to the regulation, the process of obtaining documentation/information from the Board of Management is regulated in such a way that the documentation of the minor and the data in the application form must be submitted directly to the Board of Management by the minor or his/her legal representative.In addition, the questionnaire also contains the personal data of a conscript that the school is not legally entitled or obliged to possess according to the legislation. As a result of the inspection, it was established that, contrary to the rule stipulated by the regulation, the administration obtained the personal data (such as a photograph) via the school, however, it should have been provided directly by the conscript. In this way, the conscript's personal data became available to the unauthorized persons who had neither need, nor legitimate reason or purpose to access the said data, which in turn increased the risks of unlawful data processing.

The inspection also demonstrated that data was collected directly from data subjects, including questionnaires and "communication forms". However, the Administration did not inform the data subjects to indicate the obligatory and voluntary data in the questionnaire in accordance with the rules enshrined in Article 15 of the Law of Georgia on Personal Data Protection. In addition, it was revealed that the electronic system contained the fields to be filled in (fields for psychiatrist, surgeon, therapist, ophthalmologist and others), the need for which could not be justified during inspection. At the same time, the electronic system did not fully capture all the actions taken in relation to the data existing in the electronic form (e.g., logging in/out, searching/viewing a person's personal data, opening/viewing/ copying a downloaded

document). The mentioned, in turn, increases the risks of illegal acquisition and disclosure of data, as the possibility of identifying the person responsible for illegal data processing is greatly reduced under the conditions of existing the relevant wrongful events (for example: disclosure of documents uploaded to an electronic system). Thus, by the decision of the President of Personal Data Protection Service, the District Administration as well as the City Hall of Tbilisi Municipality were imposed liability for the administrative offence envisaged by Paragraph 1 of Article 46, of the Law of Georgia "on Personal Data Protection" on the grounds of failure to comply with data protection requirements. At the same time, in order to eradicate the violations identified, the Administration as well as City Hall were given the mandatory instructions to carry out.

3. General Overview of the Basics of Data Processing

Minors indeed possess a special entitlement to personal data protection due to potentially lesser awareness of associated risks, consequences, legal safeguards, and rights in relation to their personal data processing.[174] The EU's General Data Protection Regulation (GDPR) delineates six legitimate grounds for data processing, which should be construed as comprehensive and definitive. Moreover, it's important to note that there's no hierarchical order among these bases for data processing:[175]

- Consent of the data subject;
- Fulfillment of a contractual obligation or contractual necessity;
- Fulfillment of legal obligations;
- Protection of the vital interests of the data subject or other person;
- In the public interest or to perform a public function;
- Legitimate interest of data controller or data processor or of a third party (where the interest does not outweigh the interests or fundamental right of the data subject);

The data controllers may utilize any of the aforementioned legal grounds for processing the personal data of the data subject. Furthermore, it's crucial that the processing circumstances

[174] GDPR, Recital, para. 38.

[175] Fundamentals for a Child-Oriented Approach to Data Processing, 22.

align with the mentioned legal bases. It's worth noting that certain legal bases require the data controllers to fulfill additional criteria, especially when the data subject is a minor.[176]

It's worth noting that the bases outlined in national legislation align with the legal framework of the European Union. Specifically, Article 5 of the new law sets forth the basis for data processing, including the protection of significant legitimate interests of the data controller or a third party, provided there's no prevailing interest in safeguarding the rights of minors.[177] Once more, this underscores the legislator's focus on safeguarding the best interests of minors, given their vulnerability, as evidenced by the national laws on personal data protection in many states.[178]

3.1. Consent of a Minor as a Data subject

The legal framework of the European Union institutes a two-tier protection system concerning minors. This is evidenced firstly by the obligations imposed on data controllers and secondly by the existence of special provisions regarding minors.[179] The initial paragraph of Article 6 of the General Data Protection Regulation (GDPR) of the European Union stipulates that, under subparagraph "a", the processing of personal data is lawful when "the data subject gives consent to the processing of their personal data for one or more specific purposes". Consent for data processing must be provided through a clearly expressed action, demonstrating the voluntary, specific, informed, and unambiguous agreement of the data subject to the processing of their data. This can be established, for instance, through a written statement, including the use of electronic means, or through an oral statement.[180] It's important to note that the absence of a response from the data subject, pre-checked boxes, or inactivity do not constitute consent. Furthermore, consent must encompass all processing activities conducted for the same purpose or purposes. If the data subject is required to provide consent in response to an electronic request, the request must be concise, clearly formulated, and should not impede the Service

[176] Ibid.

[177] Law of Georgia "On Personal Data Protection", date of adoption: 14/06/2023, Subparagraph "I" of paragraph 1 of Article 5.

[178] Steeves V., Macenaite M., Data Protection and children's online privacy, in: Research Handbook on Privacy and Data Protection Law, 2022, 364-365.

[179] Ibid., 367.

[180] Fundamentals for a Child-Oriented Approach to Data Processing, 22.

for which consent is sought.[181] It's crucial that the data subject has the opportunity to revoke consent.[182]

In relation to information society services (online services), the new law of Georgia "On Personal Data Protection," akin to the "GDPR," sets the age threshold for children's consent at a minimum of 16 years.[183] Imposing an age requirement for consent regarding online services does not constitute a measure aimed at preventing access to websites and applications. Additionally, it acts as an indicator for online service providers to ensure that the nature, design, and age appropriateness of their services align with the user base. Furthermore, it's important to note that in accordance with the new law of Georgia "On Personal Data Protection," digital consent obtained from individuals aged 16 or above, or in the case of minors under 16, from their parents or legal representatives, should not be utilized in a manner that treats children of all ages the same way as adults.[184]

It's crucial to acknowledge that EU Member States might impose supplementary obligations concerning the consent of minors and data protection at the domestic legislative level. Additionally, it's important to note that a controller offering cross-border services cannot always rely solely on the legislation of the Member State where it is established. It may also be required to comply with the pertinent national legislation of each Member State to which it provides services. This determination hinges on whether the Member State selects the location of the primary establishment of the data controller in its national legislation or the residence of the data subject.

It's worth considering that the existing law does not explicitly address the issue of consent by a minor, though it is bound by established legal norms governing the lawful processing of data. As per the new law "On Personal Data Protection," consent is characterized as follows: "following the provision of pertinent information to the data subject, voluntary consent expressed verbally, via telecommunication, or through other suitable means to process data pertaining to them for a specific purpose, thereby enabling the clear expression of the data

[181] GDPR, Recital, para. 32.
[182] Shudra T., "Protecting the Personal Data of Minors in the Digital Environment with Different Expectations of Parents and Children," Journal of Personal Data Protection Law, №1, 2023, 127.

[183] Law of Georgia "On Personal Data Protection", date of adoption: 14/06/2023, Article 7. It's worth noting that the "GDPR" only imposes an age limit on consent concerning the offering of electronic services. However, Georgia's new law "On Personal Data Protection" allows for the processing of personal data with the consent of a minor who has reached the age of 16.
[184] Fundamentals for a Child-Oriented Approach to Data Processing, 41.

subject's intent."[185] On the other hand, written consent pertains to "the voluntary agreement expressed by the data subject for the processing of their data for a specific purpose after receiving relevant information, which the data subject has signed or otherwise indicated in writing or in an equivalent form."[186] Article 7 of the new law addresses the processing of data concerning minors. The regulations and criteria for obtaining consent stipulate that processing data about a minor with their consent is permissible if they have attained the age of 16. In the case of an individual under 16, the consent of a parent or other legal representative is required.[187]

When offering services to children based on consent, the data controller must ensure that the user giving consent is above the age of consent, and these verification measures must be proportional to the nature and risks associated with the processing activities. In instances where users assert they have reached the digital age of consent, the data controller may conduct suitable checks to validate the authenticity of this assertion. It's important to emphasize that age verification should not result in excessive data processing. The method selected to verify the age of the data subject should entail a risk assessment of the intended processing.[188] If there are doubts, the data controller should reassess their age verification mechanisms in the specific case and contemplate the necessity of alternative verification methods.[189] It's important to highlight that, according to the new law, obtaining the consent of a parent or other legal representative is compulsory for processing data pertaining to a minor under the age of 16, ensuring it aligns with the best interests of the child.[190]Conversely, the law mandates the data controller to consider all reasonable measures to confirm the consent of the parent or legal representative.[191]Additionally, it's worth noting that consent must be given as a result of free will. For consent to be considered voluntary, the relationship between

---

[185] Law of Georgia "On Personal Data Protection", date of adoption: 14/06/2023, Subparagraph "z" of Article 2.

[186] Ibid., Subparagraph "t".

[187] It is intriguing to explore this matter within the framework of the emancipation institution, given that the Civil Code of Georgia sometimes entails full equalization of a minor's rights, such as when a person who has reached the age of 16 is granted by their legal representative the right to independently manage a business, Chanturia, L., Commentary on the Civil Code, Book I, General Provisions of the Civil Code, 2017, 70, 377.

[188] CNIL, Online age verification: balancing privacy and the protection of minors, 2022,<https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors>, [20.12.2023]; CIPL, Age Assurance and Age Verification Tools: Takeaways from CIPL Roundtable, 2023,<https://www.informationpolicycentre.com/cipl-blog/age-assurance-and-age-verification-tools-takeaways-from-cipl-roundtable>, [20.12.2023].

[189] Article 29 Working Party Guidelines on consent under Regulation 2016/679 Adopted on 28 November 2017 as last Revised and Adopted on 10 April 2018.

[190] Law of Georgia "On Personal Data Protection", date of adoption: 14/06/2023, Article 7.

[191]Ibid., Paragraph 2 of Article 7.

the data controller and the data subject must be "equal"; for instance, consent cannot be relied upon as a legal basis when there is an unequal relationship, such as between students and the school.[192] Providing information to the data subject before seeking consent is crucial to enable them to make an informed decision regarding consent.

3.2. Fulfillment of Contractual Obligation or Contractual Necessity

Data processing is lawful when it is necessary to perform a contract to which the data subject is a party or to take appropriate steps to enter into a contract requested by the data subject.[193] This legal basis is applicable when there is an actual or intended contractual relationship between the data subject and the organization. When processing a child's personal data, organizations should consider specific rules related to age restrictions and other capacities that may affect the ability to contract under national law.[194]

3.3. Fulfillment of Legal Obligation

Data processing is lawful when it is necessary to fulfil a legal obligation to which the data controller is subject.[195] Organizations can rely on this article when they are required to process personal data to meet obligations under both international and local law. When processing data on this basis, it is crucial to focus on legal obligations that arise during the processing of a child's personal data.[196] The purpose of the processing must be to fulfil the obligation. This also applies to obligations determined by public legal acts, secondary or delegated legislation, and, in specific cases, by a binding decision of a public body.[197]

3.4. Protection of the Vital Interests of the Data Subject or Another Person

[192] Swedish Authority for Privacy Protection, The rights of children and young people on digital platforms, Stakeholder guide, 22.
[193] GDPR, Article 6(1)(b).
[194] Fundamentals for a Child-Oriented Approach to Data Processing, 23.
[195] GDPR, Article 6(1)(c).
[196] Fundamentals for a Child-Oriented Approach to Data Processing, 23.
[197] Kuner Ch., Bygrave L. A., Docksey Ch., The EU General Data Protection Regulation (GDPR), A Commentary, Oxford University Press, 2020.

According to Article 6, paragraph 1, subparagraph "d" of the GDPR, data processing is lawful when it is necessary to protect the vital interests of the data subject or another natural person. This basis pertains to protecting the vital interests of the data subject or another person, such as monitoring and/or preventing the spread of an epidemic, managing humanitarian crises, and responding to natural and man-made disasters. Additionally, it should be noted that protecting the vital interests of a child may differ from those of an adult. According to the practice of the Irish Personal Data Supervisory Authority, measures to protect children take precedence over the protection of the interests of all other data subjects.[198]

3.5. In the Public Interest or to Perform a Public Function

According to Article 6, Paragraph 1, Subparagraph "e" of the GDPR, data processing is lawful when "processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller."[199] This basis for data processing typically applies to organizations performing functions mandated by public law or statutory obligations. In this context, public sector institutions have specific functions that take into account the processing of minors' data, for example: in the field of health, social care or in relation to the educational process. It should be noted that the processing must fully comply with the requirements of the legal basis, unless the public interest or the best interest of the child is counterbalanced. It should be noted that the burden of proof for the processing of minor's data is borne by the controller. [200]

3.6. Legitimate Interest of the Data Controller or Data Processor or a Third Party

"Data processing is necessary to protect the legitimate interests of the data controller or a third party, unless these interests are overridden by the interests or fundamental rights and freedoms of the data subject who requires data protection, especially if the data subject is a child."[201] The primary condition for relying on this basis is that the legitimate interests pursued by the controller do not outweigh the interests, rights, or fundamental freedoms of the data subject. This implies that the organization must evaluate the processing of a child's personal data, including identifying the legitimate interests of the data controller or organization and the

[198] Fundamentals for a Child-Oriented Approach to Data Processing, 24.
[199] GDPR, Article 6, 1(e).
[200] Fundamentals for a Child-Oriented Approach to Data Processing, 24.
[201] GDPR, Article 6, 1(f).

intended outcomes. It's crucial for the data controller or organization to demonstrate the reasons and methods behind the data processing, ensuring the use of proportionate means to achieve the legitimate purpose, and maintaining a balance between legitimate interests and the interests and fundamental rights of the child.[202]

Considering the principles outlined in international and EU legislation, the best interests of the child should serve as the primary consideration in making any decision, ensuring that the interests of the child as data subjects and/or their fundamental rights and freedoms always take precedence.[203]

3.7. Briefly About the Processing of Special Categories of Personal Data

In the context of personal data categorization, it's important to recognize the category known as "special category," or "sensitive" personal data, which is subject to specific regulations.[204] Separate grounds for processing sensitive category data are delineated by a distinct provision in the Law of Georgia "On Personal Data Protection," which establishes legal prerequisites for processing.[205] Personal data that are particularly sensitive to fundamental rights and freedoms necessitate a distinct legal protection regime[206] because the manner in which they are processed can pose significant risks to these rights and freedoms, particularly in the context of processing minors' data. The processing of such special categories of data is permissible if it ensures the protection of the rights and interests of the data subject while also being supported by a corresponding legal basis as defined by law.[207]

It's crucial that legislative regulations clearly delineate exceptional cases where the processing of special categories of data is prohibited—such as explicit consent of the data subject or for health-related purposes, including the management of public health and health services, or for archiving, scientific, historical research, or statistical research due to public interest.[208] It's noteworthy that special categories of data may be processed when the data subject has

[202] Fundamentals for a Child-Oriented Approach to Data Processing, 24.
[203] Ibid.
[204] Voigt P., Bussche A., The EU General Data Protection Regulation, A Practical Guide, 2017, 110.
[205] Law of Georgia "On Personal Data Protection", date of adoption: 14/06/2023, Article 6.
[206] Swedish Authority for Privacy Protection, Sensitive personal data <https://www.imy.se/en/individuals/data-protection/introduktion-till-gdpr/what-is-actually-meant-by-personal-data/what-is-meant-by-sensitive-personal-data/> [17.08.2023]

[207] Law of Georgia "On Personal Data Protection", date of adoption: 14/06/2023, Article 6.
[208] GDPR, Recital, para. 52.

expressly made them public, without explicitly prohibiting their use.[209] In this context, the informed decision of a minor, as a data subject, to express or disclose consent to the processing of their special category data is pertinent. A prerequisite for processing special category data of an individual under 16 is the consent of the minor's parent or legal representative, which must be based on the best interests of the child.[210] The form of consent is also a requirement for the validity of the consent, such that processing special category data of a minor is permitted only with the written consent of the parent or legal representative.[211]

3.8. Practice of the Personal Data Protection Service

- *Checking the Lawfulness of the Processing of Minor's Personal Data by the School and the Lawyer*

The legal representative of a minor (the mother) has lodged a request with the Personal Data Protection Service, seeking an examination of the lawfulness of the processing of her minor child's personal data by a public school and a lawyer. The request indicates that a civil dispute concerning the prevention of illegal trespass was deliberated in one of the district courts, with the minor as the plaintiff and a neighbor, residing in the plaintiff's vicinity, as the defendant. The neighbor had erected an ancestral cemetery in their yard without proper authorization, adversely affecting the minor's psycho-emotional well-being. Consequently, the minor's family was compelled to relocate and transfer the child to another school.

As part of the investigation, it was found that during the aforementioned court proceedings, in an effort to refute the factual circumstances presented by the plaintiff in the lawsuit, the defendant's representative submitted two written requests to the school. These requests sought evidence and information containing the minor's personal data to be presented in court. Specifically, the first correspondence requested information from the school regarding the date of the minor's enrollment and the teaching format (face-to-face or distance learning). During a subsequent letter, the representative of the defendant requested additional information, including the date of the minor's school enrollment as well as when and to which school the

[209] Law of Georgia "On Personal Data Protection", date of adoption: 14/06/2023, subparagraph "I" of paragraph 1 of Article 6.
[210] Steeves V., Macenaite M., Data Protection and children's online privacy, in: Research Handbook on Privacy and Data Protection Law, 2022, 366.
[211] Law of Georgia "On Personal Data Protection", date of adoption: 14/06/2023, paragraph 3 of Article 7.

minor moved to study. Upon inspection, it was determined that the school provided the defendant's representative with more data than requested. Furthermore, the school disclosed information about the basis for the minor's expulsion, which was subsequently presented to the court as evidence by the defendant's representative.

Based on the provided information, the Service deliberated on the lawfulness of the processing of the minor's data by both the lawyer and the school. Concerning the processing of the minor's personal data by the lawyer, the Service elucidated that the lawyer, acting within the scope of his professional duties, sought the minor's data from the school to gather evidence and present it in court, with the aim of safeguarding the interests of his client. This action was conducted in adherence to the principle of adversarial proceedings and in compliance with the requirements outlined in the Civil Procedure Code of Georgia. Within this context, the lawyer's actions served a legitimate purpose and fulfilled a specific necessity. Consequently, the Service did not ascertain any unlawful processing of the minor's personal data by the lawyer.

Regarding the lawfulness of the school's disclosure of the minor's personal data, the Service evaluated the school's action based on the grounds stipulated in Article 5, subparagraph "e" of the Law of Georgia "On Personal Data Protection" (as cited by the school). It was elucidated that, in invoking this legal basis, the school was obligated to ensure that there were no prevailing interests in protecting the rights and freedoms of the plaintiff minor in relation to those of the lawyer. Furthermore, under the circumstances where the school disclosed the minor's data to the disputing party, the educational institution couldn't ascertain the compatibility of this decision with the best interests of the child. This uncertainty arose because the institution couldn't anticipate how the further processing of the data would align with the child's interests. Based on the investigation, the Service concluded that since the school lacked the data subject's consent or a court order for data disclosure, and couldn't substantiate any other legal basis for data processing, it violated the requirements outlined in Article 5 of the Law of Georgia "On Personal Data Protection". Consequently, this violation could lead to the imposition of administrative sanctions as specified in Article 43 of the same law. Additionally, the Service highlighted that by disclosing a greater amount of data to the lawyer than was requested, the principles of data processing delineated in Article 4 of the law were also infringed upon in the aforementioned process.

- *LEPL - Center for Professional Training and Retraining of Convicts*

In order to ensure children's right to privacy, it is important to process minors' personal data, especially the one of sensitive category, in accordance with legal requirements. And if the issue concerns the disclosure of children's data, consideration should be given to how the publicized data is perceived by the third parties. In the process of disclosing juvenile data, it is especially noteworthy that publicizing of misleading information can even result in the stigmatization of a child in society. This is why, the Personal Data Protection Service of Georgia, on the basis of the request from the non-governmental organization, examined the lawfulness of minors' personal data processing by the Centre through the publication of photos on "Facebook" social network. According to the notification submitted to the Service, the information about the congratulations on Children's Day to the beneficiaries of the Monk Andrew's Charity Fund and other children suffering from oncological diseases, which was attached the identifiable photo of minors, was publicized in the form of a Facebook post.

The inspection of lawfulness of personal data processing revealed that the legal representatives of the children depicted in the photos published by the Centre and other persons had declared their consent to processing of their data. At the same time, besides the beneficiaries of the foundation (children with cancer) the photographic material showed the images of other children and family members of beneficiaries, who were at foundation for various reasons on the particular day. The information made public through "Facebook" by the Centre was therefore misleading, as according to the information indicated in the "post", the representatives of the Centre visited the beneficiaries of foundation. However, within the verification process it was stated, that together with the publicized information the photo material, posted on the social networking site by the Centre, contained the images of other persons apart from the beneficiaries as well. By decision of the President of Service, the LEPL - Centre for Professional Training and Retraining of Convicts was instructed to change the information in so called "post" in such a way, that its readers could become aware that the photos attached to the published information showed not only the beneficiaries of the fund.

4. Rights of a Minor as a Data Subject and Their Implementation

A minor is the primary beneficiary of the rights outlined in the law on personal data protection. They are entitled to and benefit from the same legal protections as adults. However, it is recommended to consider child-friendly approaches when exercising these rights. It's important to highlight that the new law "On Personal Data Protection" sets forth requirements for data controllers to establish a heightened standard of protection for the rights concerning

the processing of a child's personal data. This includes prioritizing the best interests of the child in cases where there is a disagreement between the child and their legal representative regarding data processing.[212] A notable example of child-friendly justice is the requirement to present information to the child in a format that is comprehensible to them.[213] Additionally, the new law deems the unlawful processing of data by the child as a mitigating circumstance,[214] while the unlawful processing of the child's personal data is considered an aggravating circumstance.[215] This underscores the special attention given to protecting the rights of children as data subjects. The necessity to provide specific safeguards for protecting the rights of minors arises from their unique situation, as children may have less awareness of the risks, potential consequences, rights, and legal safeguards associated with the processing of their personal data due to their age, stage of development, or level of education.[216] It's important to recognize that the rights of the data subject are not absolute and may be subject to certain limitations in exceptional cases. These rights must be exercised in balance with legitimate interests. Consequently, the rights of the data subject may only be restricted when prescribed by law and deemed necessary and proportionate in a democratic society.[217]

4.1. Right to Receive Information

"Informative self-determination necessitates the establishment of effective networks among the state, economic entities, scientific institutions, and civil society."[218] As per the applicable law, when data collection is conducted directly from the data subject, the data controller or data processor must furnish the following information to the data subject: a) the identity and registered address of data controller and data processor (if applicable); b) the purpose of data processing; c) whether the provision of data is mandatory or voluntary, along with the legal consequences of refusal if mandatory; d) the data subject's right to obtain information about the data being processed, request their rectification, update, addition, blocking, erasure , and destruction. If data collection is not carried out directly from the data subject, the data

[212] Law of Georgia "On Personal Data Protection", date of adoption: 14/06/2023, paragraph 5 of Article 7.
[213] Ibid., paragraph 5 of Article 24.
[214] Ibid., subparagraph 'b' of paragraph 1 of Article 61.
[215] Ibid., subparagraph "g" of Article 62.
[216] Hof S., Children and data protection from the perspective of children's rights – Some difficult dilemmas under the General Data Protection Regulation, 2018, 10-11. ICO, age appropriate design: a code of practice for online services, 2020, 5.
[217] Council of Europe, Modernized Convention for the Protection of Individuals with Regard to the Processing of Personal Data (Convention 108+; CM/Inf(2018)15-final), 18/05/2018, Article 11.
[218] Khubua G., Welcome Letter, Journal of Personal Data Protection Law, No. 1, 2023, 10.

controller or data processor must provide the aforementioned information upon request by the data subject.[219]

As per the updated version of the law, when gathering data directly from the data subject, data controller must furnish the data subject with at least the following information before or promptly after the data collection:

- The identity/title and contact information of the data controller, their representative, and/or the data processor (if applicable);
- Details regarding the purposes and legal basis of data processing;
- Information about the obligation to provide data, and if data provision is mandatory, explanation of the legal consequences of refusal, along with clarification that data collection/retrieval is mandated by Georgian legislation or is a prerequisite for contract conclusion (if applicable);
- Details about important legitimate interests of the data controller or a third party;
- The identity and contact information of the Personal Data Protection Officer (if appointed);
- Identification of the data recipient or categories of data recipients (if applicable);
- Information regarding the intended transfer of data and the presence of suitable data protection guarantees, including authorization for data transfer (if any), in case data controller intends to transfer data to another state or international organization;
- The duration of data storage, and if a specific duration cannot be determined, the criteria used to establish the duration;
- The rights of the data subject;[220]

If data collection is not conducted directly from the data subject, data controller is obligated to provide the data subject with the aforementioned information, along with details about which data concerning them is being processed and the source from which this data was obtained, including whether the data was acquired from a publicly available source.[221] When communicating with a child, it's crucial for the data controller to address the following issues: a) Understanding the unique characteristics of the data subject; b) Presenting information to the child in a suitable manner (such as using simple and easily understandable language or providing information in a non-written format).[222]

[219] Law of Georgia "On Personal Data Protection", date of adoption: 28/12/2011, Article 15.
[220] Law of Georgia "On Personal Data Protection", date of adoption: 14/06/2023, Article 24.
[221] Ibid., Article 25.
[222] Ibid., paragraph 5 of Article 24.

Georgian legislation and international standards mandate that data subjects must receive fundamental information regarding the intended use of their data. Ensuring clarity in this information is particularly crucial when communicating with children. The significance of providing comprehensive information is underscored in guidance documents developed by international organizations. As per the definition provided by the Article 29 Working Party, when the intended audience of the data controller comprises children or when the data controller is aware or should be aware that its product/service is predominantly utilized by minors (including situations where the data controller relies on the child's consent as the basis for processing), it is imperative to ensure that the vocabulary, tone, and language style employed are tailored to the requirements of children. This adaptation should be such that the recipient of the information can discern that the message or information is directed towards them.[223] Nevertheless, to avoid ambiguity, when providing products/services targeting young or illiterate children, transparency measures may be directed towards the parent or other legal representative. This is because such children are often unable to comprehend even the simplest written or visual communication.[224]

The child's entitlement to information regarding the processing of their personal data cannot be limited solely because consent for data processing has been granted or authorized by a parent or other representative. Even though such consent is typically provided or sanctioned by a parent or legal representative, the child, as an independent data subject, maintains an ongoing right to receive information from the data controller throughout data processing activities.[225] This aligns with Article 13 of the UN Convention on the Rights of the Child, which states that children have the right to freedom of expression, including the right to seek, receive, and impart all kinds of information and ideas.

The data controller is mandated to implement transparency measures targeted at children. This approach aligns with the guidelines set forth by the Committee of Ministers of the Council of Europe,[226] as stated in which states and other pertinent stakeholders should furnish children

[223] Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, Adopted on 29 November 2017, As last Revised and Adopted on 11 April 2018, 14 <https://ec.europa.eu/newsroom/article29/items/622227/en>, [20.12.2023].

[224] Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, Adopted on 29 November 2017, As last Revised and Adopted on 11 April 2018, para. 15.

[225] Ibid., para. 15.

[226] See, CoE, Guidelines to Respect, Protect and Fulfil the Rights of the Child in the Digital Environment, Recommendation CM/Rec(2018)7 of the Committee of Ministers, <https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a>, [20.12.2023]. See, also, CoE, Recommendation CM/Rec(2012)2 of the Committee of Ministers to member States on the Participation of Children and Young

with information about their rights, including participation rights, using a language comprehensible to them and suitable for their level of development and prevailing circumstances. Opportunities should be established for children to express themselves via information and communication technologies. Children must be educated about mechanisms and services that offer appropriate support and procedures for lodging complaints, seeking remedies, or addressing violations of their rights. This information should also be accessible to their parents or legal representatives, enabling them to aid children in exercising their rights.[227] Additionally, both the child and their representative should receive supplementary information about the procedures for exercising the right to object to data processing.[228]

4.2. Right to Request Information

The exercise of the right of access pertains solely to the personal data belonging to the data subject and involves two stages: Firstly, the controller must ascertain whether the personal data of the data subject is indeed being processed; and secondly, if such processing is underway, the data subject must be granted access to the following information: the purposes of the processing; categories of processed personal data; recipients or categories of recipients; planned duration of storage or criteria for determining it. Additionally, the data subject must be informed of their rights, such as rectification, erasure, or restriction of processing, as well as their right to appeal. Furthermore, if the data is not collected directly from the data subject, the data subject must be provided with information about the source of the data.[229]The controller is obligated to ensure the realization of the right of access while also safeguarding the rights and freedoms of others adequately.[230]

As per the preamble of the Guideline Recommendation of the European Data Protection Board (EDPB) on the right of access of the data subject, the General Data Protection Regulation

---

People under the Age of 18, <https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805cb0ca>, [20.12.2023].

[227] CoE, Guidelines to Respect, Protect and Fulfil the Rights of the Child in the Digital Environment, Recommendation CM/Rec(2018)7 of the Committee of Ministers, para. 6, <https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a>, [20.12.2023].

[228] Ibid., para. 33. Committee on the Rights of the Child, General Comment No. 12 (2009) The Right of the Child to be Heard, para 25, <https://www2.ohchr.org/english/bodies/crc/docs/advanceversions/crc-c-gc-12.pdf>, [20.12.2023].

[229] GDPR, Intersoft Consulting, Right of Access, <https://gdpr-info.eu/issues/right-of-access/>, , [20.12.2023].

[230] Definition of the scope of the right by the Irish supervisory authority, <https://www.dataprotection.ie/en/individuals/know-your-rights/right-access-information>, [20.12.2023].

(GDPR) of the European Union emphasizes[231] that the data subject's right to receive a copy of their processed personal data (based on processing activities, categories of personal data, etc.) should not impinge upon the rights and freedoms of others. The EDPB asserts that considerations regarding the rights and freedoms of others should be taken into account not only when sharing information through providing a copy but also when granting access through other means. Additionally, the data controller must be capable of evaluating whether, in a specific case, exercising the right of access would detrimentally impact the rights or freedoms of others.[232]

According to the current law "On Personal Data Protection," the data subject possesses the right to be informed by the data controller about their personal data and to obtain copies of said data free of charge.[233] The objective of the right to request information and receive a copy is to furnish data subjects with adequate, transparent, and readily accessible information regarding their personal data and its processing. This enables the data subject to comprehend and ascertain the lawfulness of the processing and the accuracy of the processed data. The right to request information and receive a copy serves to facilitate the exercise of other rights, including the right to erasure or rectification. According to the definition provided by the European Court of Human Rights (ECTHR), states bear a positive obligation to guarantee the due respect for privacy and establish effective and accessible procedures enabling the data subject to obtain all pertinent and suitable information.[234] Additionally, it is important to note that the data subject is not required to justify their request.[235] Furthermore, the data controller must evaluate whether the request pertains to all processed data concerning the data subject or only a portion thereof.[236] The data subject retains the right to send a request to the official address of the data controller, rather than utilizing the communication channels specified by the controller. [237] Additionally, the methods of granting access to data may differ based on the

[231] GDPR, Artcile 15(4): "The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.", <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e2599-1-1>, [20.12.2023].

[232] EDPB, Guidelines 01/2022on data subject rights - Right of Access, 18.01.2022, <https://edpb.europa.eu/system/files/2022-01/edpb_guidelines_012022_right-of-access_0.pdf>, [20.12.2023].

[233] Law of Georgia "On Personal Data Protection", date of adoption: 28/12/2011, Article 21, the issue is basically similar to the new law under Article 14.

[234] See, ECtHR, Roche v. the United Kingdom [GC], 2005, § 162; Haralambie v. Romania, 2009, § 86; Joanna Szulc v. Poland, 2012, §§ 86, 94.

[235] EDPB, Guidelines 01/2022 on Data Subject Rights - Right of Access, Adopted on 28 March 2023, 3, <https://edpb.europa.eu/system/files/2023-04/edpb_guidelines_202201_data_subject_rights_access_v2_en.pdf>, [20.12.2023].

[236] Ibid., 3.

[237] Kuner Ch., Bygrave L. A., Docksey Ch., The EU General Data Protection Regulation (GDPR), A Commentary, Oxford University Press, 2020, art. 15, 465.

volume of data and the complexity of the processing operations conducted. In the absence of specific instructions in the request, a request for access to data is presumed to encompass access to all personal data concerning the data subject. However, if the data controller manages a substantial amount of data, they may request the data subject to specify the scope of the request.[238] It's important to highlight that the extent of exercising the right of access to data is delineated by the concept of personal data. Data subjected to pseudonymization, unlike depersonalized data, still retains its status as personal data. The right to access data pertains to the personal data of the individual making the request. Consequently, it shouldn't be narrowly interpreted, and the right to access data may encompass information regarding third parties, such as communication history, encompassing both incoming and outgoing messages.[239]

In accordance with international practice, the data controller reserves the right to decline the execution of requests deemed clearly unreasonable or excessive, or to impose a reasonable fee for such requests. It's noteworthy that if a fee is charged to the data subject, the controller must be capable of demonstrating the clearly unreasonable or excessive nature of the request.[240]

When a parent or legal representative exercises the right of access to data on behalf of a minor, it's essential to prioritize the best interests of the child as the primary consideration in determining whether to exercise the right to access personal data. Furthermore, it is recommended that the data controller implements suitable technical or organizational measures to prevent any unauthorized disclosure of personal data of minors, thereby averting unauthorized access. However, it's worth noting that national legislation may stipulate the right of a parent or legal representative to request and receive information concerning a minor (such as details regarding the child's academic performance and assessments).[241]

4.3. Right to Request Rectification, Update or Completion of Data

As per current legislation, the data controller is required to rectify, update, complete, to, block, erase, or destroy data upon the data subject's request if the data is incomplete, inaccurate, outdated, or if its collection and processing were conducted unlawfully.[242]

---

[238] Ibid., 4.

[239] Ibid.

[240] Kuner Ch., Bygrave L. A., Docksey Ch., The EU General Data Protection Regulation (GDPR), A Commentary, Oxford University Press, 2020, art. 15, 466.

[241] EDPB, Guidelines 01/2022 on Data Subject Rights - Right of Access, Adopted on 28 March 2023, paras. 83-87, <https://edpb.europa.eu/system/files/2023-04/edpb_guidelines_202201_data_subject_rights_access_v2_en.pdf>, [20.12.2023].

[242] The Law of Georgia "On Personal Data Protection," adopted on December 28, 2011, Article 22, in its current edition, groups together rights of different natures. However, the new law "On Personal Data Protection" does

In the latest iteration of the law, the data subject possesses the rights to update, rectify, and complete data (known as the right to data rectification).[243] This aligns closely with the principle of data accuracy and updating, compelling the data controller to promptly erase or destroy inaccurate data without undue delay.[244] The controller is mandated to inform all recipients of data, as well as other data controllers for the same data and data processors, to whom the data was transferred, about any updates and additions to the data, unless it is impracticable due to the number of controllers, processors, or recipients of data, and/or due to disproportionately high costs. Upon receiving this information, the aforementioned individuals are obligated to rectify, update, and/or complete the data within a reasonable timeframe. This provision affords the data subject the opportunity to prevent the dissemination of inaccurate or false personal data about them.[245]

The right to data rectification serves as an embodiment of the data subject's power to manage data pertaining to them, encompassing data quality control. This right is intricately linked to the exercise of the data subject's right of access. Without access to their own data, the data subject would be unable to evaluate the accuracy, completeness, or necessity of updating the processed personal data.

It is noteworthy that the right to data rectification was among the earliest rights conferred upon data subjects in international legal frameworks concerning data protection. Article 8, subparagraph “c” of the Council of Europe Convention for the “Protection of Individuals with regard to Automatic Processing of Personal Data” (Convention 108) stipulates that individuals should be afforded the opportunity, to the extent possible, to rectify personal data concerning them if such data have been processed contrary to the fundamental principles of data protection. As per the convention's definition, rectification entails correcting "false or irrelevant information."[246]

---

not adopt this approach. This paper considers the approach of the new edition of the law, consolidating the contents of one type of rights together.

[243] Law of Georgia "On Personal Data Protection", date of adoption: 14/06/2023, Article 15.

[244] Law of Georgia "On Personal Data Protection", date of adoption: 14/06/2023. Article 4, paragraph 1, subparagraph "d". The principle of accuracy is also provided for by Article 4 of the current legislation.

[245] Law of Georgia "On Personal Data Protection", date of adoption: 14/06/2023, Article 15.

[246] CoE, Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28.I.1981, para. 54, <https://rm.coe.int/16800ca434#:~:text=The%20object%20of%20this%20convention,of%20computers%20for%20administrative%20purposes>, [20.12.2023].

As previously mentioned, the right to data rectification encompasses the right to complete incomplete information, which is determined by the purpose of data processing. Depending on the objective of data processing, the same dataset may be deemed both complete and incomplete. Filling incomplete data involves adding the missing portions to the dataset. For instance, such a scenario may arise in relation to expungement of a criminal conviction.[247]

The European Court of Human Rights ("ECtHR") has ruled in numerous cases that the storage and dissemination of personal data, without affording the data subject the opportunity to refuse its processing, constitutes an infringement upon the right to respect for private life.[248] The Court has determined that a state party to the European Convention on Human Rights has a positive obligation, upon submission of pertinent evidence by individuals, to rectify personal data pertaining to said individuals.[249] The court highlighted that not only retaining false or inaccurate information but also providing incomplete information to third parties (such as failing to mention the applicant's acquittal) amounts to a violation of the right to privacy.[250]

The Court of Justice of the European Union ("CJEU") has examined the right to data rectification in several cases. The court has associated the right to data rectification with the fundamental right to an effective legal remedy, emphasizing that the essence of this fundamental right remains unprotected if individuals do not have the opportunity to seek legal remedies to access their personal data and request the rectification or erasure of such data.[251]

The European Court of Justice also examined the right to request access to personal data concerning the candidate's written responses to examinations and any annotations made by examiners on these documents, on the basis that such documents were likely subject to the right to data rectification. The court deemed this data to be personal data and clarified that the applicant was entitled to access the test responses to verify if any technical errors had occurred (such as errors in marking), although this did not imply rectifying incorrectly answered tests.[252]

The essence of the aforementioned approach is aptly elucidated in preamble paragraph 47 of the 2016 EU directive on the processing of personal data in the police sector. It states that the right to rectification pertains to facts; specifically, opinions cannot be labeled as accurate or

[247] Kuner Ch., Bygrave L. A., Docksey Ch., The EU General Data Protection Regulation (GDPR), A Commentary, Oxford University Press, 2020, art.16, 473.
[248] ECtHR, Leander v Sweden, para. 48; ECtHR, Rotaru v Romania, para. 46.
[249] ECtHR, Ciubotaru v Moldova, paras. 58–59.
[250] ECtHR, Cemalettin Canli v Turkey, paras. 41–42.
[251] CJEU, Case C-362/14, Schrems, para. 95.
[252] CJEU, Case C-434/16, Nowak, para. 49.

inaccurate, whereas facts can be either true or false. Therefore, factual circumstances rather than opinions are subject to rectification.[253]

The importance of the right to rectification of data is underscored in the recommendation of the Committee of Ministers of the Council of Europe regarding the protection of children's rights in the digital environment. According to the recommendation, states should guarantee that children and/or their parents, guardians, or legal representatives have the right to withdraw consent to data processing, to access their personal data, and to rectify or erasure it, particularly in cases where the data processing is unlawful or poses a threat to the dignity, safety, or privacy of the data subject, especially minors.[254]

4.4. Right to block data

Article 22 of the current legislation delineates, among other rights of the data subject, the right to request the blocking of personal data processing.[255] In a comparative context, it's noteworthy that according to Article 17 of the new law, the data subject also holds the right to request the data controller to block the data under certain circumstances: a) when the data subject disputes the validity or accuracy of the data; b) when data processing is unlawful, yet the data subject opposes their erasure and requests data blocking; c) when the data are no longer necessary for the intended purpose of processing, but the data subject requires them for filing a complaint or lawsuit; d) when the data subject requests the cessation, erasure, or destruction of data processing, and this request is under consideration; e) when data need to be retained for evidentiary purposes. Consequently, the data controller is obligated, upon the data subject's request, to block the data if one of the aforementioned conditions is met, except in cases where circumstances stipulated by law dictate otherwise.[256]

It's crucial to clarify that data blocking entails halting all feasible actions related to personal data processing, with the exception of data storage. The right to data blocking serves as a supplementary right in relation to other fundamental rights concerning data processing (such

[253] Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, recital 47, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680>, [20.12.2023].

[254] CoE, Guidelines to Respect, Protect and Fulfil the Rights of the Child in the Digital Environment, Recommendation CM/Rec(2018)7 of the Committee of Ministers, para. 34, <https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a>, [20.12.2023].

[255] Law of Georgia "On Personal Data Protection", date of adoption: 28/12/2011, Article 22.

[256] Law of Georgia "On Personal Data Protection", date of adoption: 14/06/2023, Article 17.

as the right to data rectification or the right to object to data processing).[257] In the case of "*College van burgemeester en wethouders van Rotterdam v M.E. E. Rijkeboer*," the European Court of Justice deliberated on both the scope of the right to access data while on the other hand, there's the burden of the obligation imposed on the data controller to retain data that they are not entitled to use for other purposes. In this decision, the Court ruled that member states must uphold a fair balance between the interests of the data subject and the burden imposed on the data controller concerning the retention of information.[258]

According to the practice of the European Court of Justice, the data subject can, relying on Articles 7 and 8 of the "Charter of Fundamental Rights of the European Union" and considering their fundamental rights, request that certain data no longer be accessible to the general public, including data not being indexed by internet search engines. Additionally, in one case, the court defined methods of data blocking as follows: a portion of the data was made inaccessible to users, and the published data was temporarily removed from the website.[259]

4.5. Right to Request Erasure and Destruction of Data

The "right to be forgotten" entails the data subject's request to erase specific data. Furthermore, under particular circumstances, the data subject can request the operator of an online search engine to remove from search results the URLs leading to the internet source containing the personal data.[260] The rights of erasure, akin to those in the new law, are also provided for in the current legislation.[261] In accordance with the new law, the data subject possesses the right to request the data controller to cease, erasure, or destroy data processing (including profiling). It's important to highlight that the "right to be forgotten" is not absolute and is not unconditionally guaranteed, particularly when it conflicts with the freedom of expression of

[257] European Commission, When should I exercise my right to restriction of processing of my personal data? <https://commission.europa.eu/law/law-topic/data-protection/reform/rights-citizens/my-rights/when-should-i-exercise-my-right-restriction-processing-my-personal-data_en>, [20.12.2023].
[258] CJEU, Case C-553/07, Rijkeboer, para. 64.
[259] Case C-131/12, Google Spain, para. 99.
[260] Bernsdorf B., Search engine operators and the “right to be forgotten”, Journal of Personal Data Protection Law, No. 1, 2023, 55.
[261] Law of Georgia "On Personal Data Protection", date of adoption: 28/12/2011, Article 22.

the information society and the right to information.[262] Consequently, the data controller has the right to refuse to fulfill the request if:

- There is any legal basis for data processing;
- The data is processed to substantiate a legal claim or defending a response;
- Data processing is necessary for exercising the right to freedom of expression or information;
- The data is processed for archiving purposes in the public interest, as prescribed by law, for scientific or historical research, or statistical purposes, and halting, erasing, or destroying the data processing would render it impossible or significantly impair the attainment of the processing objectives.[263]

Paragraph 65 of the preamble of the General Data Protection Regulation (GDPR) elucidates the right to be forgotten for data subjects, underlining its particular significance concerning minors. It specifies that the data subject has the right to have their personal data erased and no longer subject to processing if the data are no longer necessary for the purposes for which they were collected or processed, if the data subject withdraws consent or objects to the processing of personal data, or if the processing of their personal data contravenes the provisions of the GDPR. This right holds particular relevance when the data subject consented to data processing during childhood without a proper assessment of the associated risks. Nonetheless, it's important to note that continued storage of personal data is lawful in instances where it is necessary to exercise the right to freedom of expression and information, to fulfill legal obligations, to meet duties imposed in the public interest, and depending on other circumstances.[264]

For the effective implementation of the right to erasure in the digital realm, it should be interpreted broadly, requiring the data controller who has published personal data to inform other controllers about all links, copies, or replicas of the data subject to be erased. Consequently, the controller must, considering the available technologies and means at their disposal, take all reasonable measures to inform other data controllers about the data subject's request.[265]

The right to erasure is also enshrined in Article 8(c) of the Council of Europe Convention for the "Protection of Individuals with regard to Automatic Processing of Personal Data"

[262] Bernsdorf B., Search engine operators and the "right to be forgotten", Journal of Personal Data Protection Law, No. 1, 2023, 55.
[263] Law of Georgia "On Personal Data Protection", date of adoption: 14/06/2023, Article 16.
[264] Kuner Ch., Bygrave L. A., Docksey Ch., The EU General Data Protection Regulation (GDPR), A Commentary, Oxford University Press, 2020, art. 17, 475-476.
[265] Ibid., 476.

(Convention 108). This provision grants the data subject the right to request the rectification or erasure of data if the processing of such data contravenes domestic law, thereby ensuring the enforcement of the fundamental principles outlined in Articles 5 and 6 of Convention 108.[266]

In the case "W*ęgrzynowski and Smolczewski v Poland*," the European Court of Human Rights (ECtHR) deliberated on and addressed the "right to be forgotten" of the data subject. The case revolved around the removal of an article about the applicant from the archive of a specific newspaper's website, following a determination that the publication of the article had infringed upon the applicant's rights. The ECtHR faced the challenge of balancing the freedom of expression, particularly the freedom of the press, with the applicant's right to privacy. The European Court determined that an appropriate measure to safeguard the applicant's rights would be to append a comment to the article on the website, providing the public with information regarding the Court's decisions. According to the Court's interpretation, completely removing the article from the archive might be akin to rewriting history, which would conflict with the legitimate interest of the public in accessing public internet archives of the press, a right protected by Article 10 of the European Convention on Human Rights.[267] Additionally, it's noteworthy that the European Court of Human Rights also considers the right to erasure of data in relation to the following issues:

- The practice of media outlets maintaining long-term archives on their websites containing personal data of individuals, such as last name, first name, and photo, that have been published in the past;[268]
- The possibility for individuals accused or suspected of having committed a crime to obtain, after a certain period, the right to erase personal data collected by authorities (such as DNA profiles, identity photos, and fingerprints) from databases designed for preventing and combating crime;[269]
- The inability of an individual to request the erasure of their previous conviction from police archives after a certain period of time;[270]

[266] CoE, Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28.I.1981, Para. 54, <https://rm.coe.int/16800ca434#:~:text=The%20object%20of%20this%20convention,of%20computers%20for%20administrative%20purposes>, [20.12.2023].

[267] ECtHR, Węgrzynowski and Smolczewski v Poland, paras. 65 and 66.

[268] ECtHR, M.L. and W.W. v. Germany, 2018.

[269] ECtHR, B.B. v. France, 2009; Gardel v. France, 2009; M.B. v. France, 2009; M.K. v. France, 2013; Brunet v. France, 2014; Ayçaguer v. France, 2017; Catt v. the United Kingdom, 2019; Gaughran v. the United Kingdom, 2020.

[270] ECtHR, M.M. v. the United Kingdom, 2012.

– The extended retention of applicants' personal data in the archives of the Security Service, which no longer fulfilled the criterion of "necessity in a democratic society," considering the nature of the action and the age of the applicant;[271]

It is worth mentioning that in the case "M.M. v. the United Kingdom," the European Court of Human Rights found a violation of Article 8 of the Convention due to the lifelong registration of a warning against an individual in the police record.[272] According to the court's rationale, past punishment served or warnings received gradually become ingrained in the personal life of the individual who committed the act. While data in criminal databases could be considered public information to some extent, their systematic storage in central files meant that the data could be disclosed long after the event, when everyone except the data subject had forgotten about the incident. The court expressed concern over the highly restrictive criteria for data erasure and noted that requests for erasure were permitted only in exceptional cases.[273] The Court concluded that when a state exceeds the bounds of discretion in data retention by utilizing its powers extensively, such as imposing indefinite data retention, it is essential to have effective safeguards to ensure the erasue of data when their retention is no longer compatible with a legitimate purpose.[274]

The landmark decision of the Court of Justice of the European Union (CJEU) concerning the right to erasure is the "Google Spain" case. In this case, a Spanish citizen requested Google Spain to remove links to two publications from a Spanish newspaper from the search engine results list associated with his name. Based on the mentioned publications, an order from the Ministry of Spain announced a real estate auction related to the removal of social security debts, specifying the name of the individual.[275]According to the court's interpretation, safeguarding the rights of the data subject takes precedence over other interests. However, in certain instances, the interests of the general public may outweigh those of the data subject. The court elaborated that this determination hinges on the nature of the particular information, its effect on the personal life of the data subject, and the public interest in possessing such information. The significance of the interest may vary depending on the public role of the data subject and their involvement in public affairs.[276]

[271] ECtHR, Segerstedt-Wiberg and Others v. Sweden, 2006.
[272] ECtHR, M.M. v. the United Kingdom, 2012, §§187-207.
[273] Ibid., § 202.
[274] ECtHR, Catt v. the United Kingdom, 2019, § 119; Gaughran v. the United Kingdom, 2020, § 94.
[275] Case C-131/12, Google Spain.
[276] Case C-131/12, Google Spain, paras. 81 and 97.

4.6. Right to Withdraw Consent

The data subject retains the right, at any time and without providing justification, to withdraw consent previously granted and to request the cessation of data processing and/or the destruction of processed data.[277] According to Georgian legislation, the data subject has the right to withdraw their consent at any time, without explanation or justification. In this case, at the request of the data subject, data processing must be stopped and/or the processed data must be erasured or destroyed no later than 10 working days after the request, provided there is no other reason for the data processing.The data subject has the right to withdraw consent in the same manner in which consent was initially given. Furthermore, prior to withdrawing consent, the data subject has the right to request and receive information from the data controller about the potential consequences of withdrawing consent.[278] It's crucial that the data controller informs the data subject about this right before seeking consent. Withdrawing consent should be as straightforward as granting consent. For instance, if consent is provided electronically, it should also be possible to withdraw it through equally suitable means. Withdrawing consent does not imply that the data processing carried out before the withdrawal was unlawful. It's important to note that if the data controller has another lawful basis for data processing, the withdrawal of consent does not necessarily halt data processing. Personal data that has been lawfully processed based on consent does not need to be erasured unless another legal basis exists.[279] However, in such cases, the data subject must be informed of the change in the legal basis for data processing.[280] The data controller must clearly distinguish, at the beginning of data processing, the purpose and legal basis on which the data processing is based.[281] According to the guideline recommendation of the European Data Protection Board, when the data subject gives consent and the data controller intends to continue processing the personal data based on another legal basis, the controller must inform the data subject about the change in the legal basis of the data processing.[282]

To facilitate the revocation of consent for a service provided through a specific user account (e.g., via a website, application, authorization, "Internet of Things" (IoT) interface, or email), the data subject should have the ability to withdraw consent without any harm through the

[277] Law of Georgia "On Personal Data Protection", date of adoption: 28/12/2011, Article 25.
[278] Law of Georgia "On Personal Data Protection", date of adoption: 14/06/2023, Article 20.
[279] Kuner Ch., Bygrave L. A., Docksey Ch., The EU General Data Protection Regulation (GDPR), A Commentary, Oxford University Press, 2020, art. 7, 351.
[280] Ibid.
[281] Ibid., paras. 115-118.
[282] Ibid., para. 120.

same electronic means, as withdrawing consent through other means might entail excessive effort. The data controller must ensure that revoking consent is free of charge and does not result in a reduction in the quality of service.[283]

It's noteworthy that the new law introduces specific provisions regarding the acquisition of consent from children as data subjects.[284] Since withdrawing consent to data processing is a critical aspect of informed and freely given consent, additional safeguards are also applied to the withdrawal of consent to protect children's rights.

4.7. Right to Data Portability

According to Article 18 of the new law, in cases of automated data processing under the provisions outlined in Article 5, paragraph 1, subparagraphs "a" and "b",[285] and Article 6, paragraph 1, subparagraph "a",[286] the data subject has the right to receive the data they provided in a structured, commonly used, and machine-readable format from the data controller or to request the transfer of this data to another data controller, if technically feasible. The right to data portability aims to facilitate the data subject in transferring, copying, or easily moving their personal data from one IT system to another (whether it be the data subject's own protected systems, a trusted third party, or new data controllers).[287]

The main elements of the right to data portability include: the right to receive personal data; the right to transfer personal data from one data controller to another; and control over data processing.[288]

---

[283] EDPB, Guidelines 05/2020 on consent under Regulation 2016/679, 2020, para. 114, <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf>, [20.09.2023].

[284] Law of Georgia "On Personal Data Protection", date of adoption: 14/06/2023, Article 7.

[285] Data processing is permissible if one of the following grounds is met: a) The data subject has provided explicit consent for the processing of their data for one or more specific purposes. b) Data processing is considered necessary to fulfill an obligation arising from a deal entered into with the data subject or to initiate a deal at the request of the data subject.

[286] The processing of special category data is permissible only if the data controller ensures the guarantees specified by this law for protecting the rights and interests of the data subject, and if one of the following grounds is met: a) The data subject has provided written consent for the processing of special category data for one or more specific purposes.

[287] Article 29 Data Protection Working Party, Guidelines on the right to data portability, 2017, 4, <https://ec.europa.eu/newsroom/article29/items/611233>, [20.09.2023].

[288] Ibid., 4-6.

The right to receive personal data - particularly the right to data portability, entails the data subject's entitlement to receive a subset of personal data processed by the data controller, which pertains to them, and to retain this data for subsequent personal use. Such storage can be achieved using personal devices or private cloud servers, without the necessity of transferring the data to other data controllers. In this regard, the right to data portability complements the right to access data. One notable aspect of data portability is that it provides an effortless method for data subjects to manage and reuse their personal data.[289]

The right to transfer personal data from one data controller to another - this right empowers data subjects to transfer their personal data from one data controller to another seamlessly and without obstacles. Data can also be directly transferred from one data controller to another at the data subject's request, provided it is technically feasible to do so. It is recommended that controllers develop compatible formats that allow for data portability without obligating the controller to implement or maintain technically compatible processing systems. This element of the right to data portability not only enables data subjects to obtain and reuse their data but also to transfer the data they receive to other service providers.[290]

Control - The right to transfer data ensures that data subjects have the right to receive their personal data and process it according to their preferences. Data controllers handling data portability requests are not accountable for the data processing performed by the data subject or by other recipients of the personal data.[291] They act on behalf of the data subject, even when the personal data is directly transferred to another data controller. In this context, the data controller is not liable for ensuring the compliance of processing activities conducted by the recipient with data protection legislation, as the data recipient is not selected by the data sender. However, the data controller must implement measures to guarantee that they are truly acting on behalf of the data subject. For instance, they may establish procedures to verify that the personal data transferred accurately reflect the content and format desired by the data subject. This verification can be achieved by obtaining confirmation from the data subject before transferring the data, by obtaining initial consent for processing, or by incorporating relevant contractual terms.[292]

[289] Ibid., 4-5.
[290] Ibid., 5.
[291] Kuner Ch., Bygrave L. A., Docksey Ch., The EU General Data Protection Regulation (GDPR), A Commentary, Oxford University Press, 2020, art. 20, 504-505.
[292] Article 29 Data Protection Working Party, Guidelines on the right to data portability, 2017, 6, <https://ec.europa.eu/newsroom/article29/items/611233>, [20.09.2023].

Enforcing the genuine intent of the data subject is particularly crucial when it comes to children, as the data controller has additional responsibilities regarding defining the scope of the right and implementing it in a manner comprehensible to minors.

4.8. Automated Individual Decision-Making and Related Rights

According to Article 19 of the new law, the data subject retains the right not to be subjected to a decision made solely through automated means, including profiling, if this decision produces legal or significant effects for them. However, exceptions to this rule include situations where the profiling decision is based on the explicit consent of the data subject, which is necessary for the conclusion or performance of a contract between the data subject and the data controller, or if such profiling is mandated by law or subordinate regulations issued under delegated authority based on the law.

Profiling and automated decision-making are prevalent in both private and public sectors. Technological advancements, particularly in big data analytics, artificial intelligence, and machine learning, have enabled the creation of profiles and the adoption of automated decisions that can greatly influence the rights and freedoms of individuals.[293] The widespread availability of personal data online and the use of "Internet of Things" (IoT), the capacity to identify correlations and draw connections enables the identification, analysis, and prediction of aspects of an individual's personality traits, behaviors, interests, and habits.[294]

While profiling and automated decision-making offer benefits in terms of efficiency and resource savings[295] for both individuals and organizations, they also pose risks to the rights and freedoms of individuals, necessitating the implementation of adequate safeguards. According to the 29th Working Group Guidelines, profiling can sometimes result in inaccurate predictions and, in other instances, lead to denial of service and unjustified discrimination.[296]

Profiling is a process that may entail statistical deductions. It is commonly employed to predict outcomes about individuals, utilizing data from various sources to infer characteristics of an individual based on other statistically similar traits.[297] In essence, profiling involves collecting

[293] Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 2018, 5, < https://ec.europa.eu/newsroom/article29/items/612053/en >, [20.09.2023].
[294] Ibid.
[295] Ibid.
[296] Ibid., 6.
[297] Ibid., 7.

information about an individual or a group of individuals and assessing their characteristics or behavioral patterns, categorizing them for purposes such as analytical assessment and/or making preliminary predictions regarding matters like task performance ability, interests, or probable behavior.[298]

It's crucial to distinguish that automated decision-making encompasses a different scope compared to profiling and may partially overlap or coincide with it. Automated decision-making specifically refers to the capacity to make decisions using technological means without human intervention. Automated decisions can be based on various types of data, including data provided directly by individuals (such as questionnaire responses); observational data (such as location data collected through applications); and inferential data (such as existing individual profiles like credit scores).[299] It's important to note that automated decisions can occur with or without profiling, and profiling can take place independently of automated decision-making. However, it's also possible for a straightforward automated decision-making process to be based on profiling.[300]

Protecting the personal data of minors is of paramount importance, especially in the context of fully automated decision-making and profiling. The General Data Protection Regulation imposes additional responsibilities on data controllers when processing the personal data of minors.[301] According to the preamble paragraph 71 of the regulation, automated decision-making, including profiling, with legal or similarly significant effects, must not be applied to children. Since the mentioned wording isn't explicitly mirrored in the pertinent article of the General Data Protection Regulation, the Article 29 Working Party doesn't interpret Article 71's reservation as an absolute ban on this kind of processing concerning children.[302] Article 22 of the Regulation does not prohibit automated decision-making concerning a child unless it results in legal or similarly significant effects on the child.[303] In cases involving automated decision-making or profiling of children, appropriate safeguards must be in place, in line with the best interests of minors. The data controller is responsible for ensuring the effectiveness of these safeguards to protect the rights, freedoms, and legitimate interests of children as data subjects.[304]

---

[298] Ibid.
[299] Ibid., 8.
[300] Ibid.
[301] GDPR, Recital, para. 71.
[302] Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 2018, 28, < https://ec.europa.eu/newsroom/article29/items/612053/en >, [20.09.2023].
[303] Ibid., 29.
[304] Ibid., 28.

Given that children constitute a more vulnerable segment of society, organizations should generally avoid profiling them for marketing purposes. Children can be especially sensitive in the online realm and more susceptible to the influence of behavioral advertising. For instance, profiling in online gaming can be utilized to target players who, based on the algorithm, are deemed more inclined to make in-game purchases. A child's age and developmental stage may impact their capacity to comprehend the motivations or ramifications of this form of marketing.[305]

4.9. Right to Appeal

The data subject retains the right to lodge a complaint with the personal data protection Service[306] or seek recourse through the court in the event of a violation of their rights. If the entity responsible for data processing is a public institution, a complaint can also be filed with the same or a higher administrative body. The President of the Personal Data Protection Service assesses the data subject's application in accordance with relevant laws and normative acts.[307]

The Personal Data Protection Service serves as an independent supervisory body for data protection, tasked with ensuring the lawfulness of personal data processing in Georgia. The Data Protection Supervisory Authority is an independent public body, it oversees the enforcement of data protection laws, monitors the lawfulness of personal data processing, and implements preventive measures as necessary. Moreover, this supervisory body offers consultations and reviews complaints concerning infringements of data protection legislation.[308]

In the international legal landscape, it's notable that the updated Council of Europe Convention "On the Protection of Individuals with Regard to the Processing of Personal Data" (Convention 108+) acknowledges the data subject's right, when exercising the rights outlined in the Convention, to seek assistance from the supervisory authority, irrespective of their

[305] Ibid., 29.
[306] For more information, see the official website of the Personal Data Protection Service: <www.personaldata.ge>.
[307] Law of Georgia "On Personal Data Protection", date of adoption: 28/12/2011, Article 26.
[308] European Commission, What are Data Protection Authorities (DPAs), <https://commission.europa.eu/law/law-topic/data-protection/reform/what-are-data-protection-authorities-dpas_en>, [20.12.2023].

nationality and place of residence.[309] Additionally, under the European Union's General Data Protection Regulation (GDPR), supervisory authorities are mandated to implement measures that facilitate the submission of complaints in an electronically fillable format, while not precluding other modes of communication.[310]

4.10. Practice of the Personal Data Protection Service

- *Inspection of LEPL - Agency for State Care and Assistance for the Victims of Human Trafficking*

The Personal Data Protection Service reviewed the lawfulness of the LEPL - Agency for State Care and Assistance for Victims of Human Trafficking (hereinafter - the Agency) informing a minor under state care, prompted by the minor's application.

During the examination of the application, it was determined that, with the minor's consent, their representative submitted two written requests to the agency for information and documentation concerning the minor. The first request sought information about the reasons for the minor's change of residence, the services provided to them, and documentation containing the minor's data. The second request pertained to additional information regarding the minor's departure from a specific small family home during a certain period.

In reply to the requests, the agency notified the minor's representative in writing on both occasions that the requested information and documentation would be furnished after seeking and obtaining information from the pertinent regional centers. Eventually, the agency supplied the representative with the complete requested information and documentation. However, this action curtailed the data subject's (minor's) right to receive the requested information within the statutory 10-day timeframe.

During the review of the application, it was determined that the agency needed to gather information from its various divisions to furnish the requested information and documentation. As explained by the agency's social worker, details regarding the services rendered to the minor in state care are managed by social workers handling the case of each respective minor. However, due to their overloaded schedules, acquiring this information

[309] CoE, Convention 108 +, Convention for the Protection of Individuals with regard to the Processing of Personal Data, 2018, Article 18, <https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1>, [20.12.2023].
[310] GDPR, Article 57 (2).

posed a challenge.Taking into account the time and workload constraints of social workers, the delivery of documentation to the data subject may encounter delays depending on the priorities of other individuals (beneficiaries). According to the agency, fulfilling the information request from the minor's representative necessitated the collection, analysis, and processing of documents housed in various regional centers. This task couldn't be completed promptly or within the 10-day timeframe, given the limited resources of social workers and the requirement to gather data from multiple institutions. In this case, considering the structural features of social work and the agency, its specific competencies, the information provided during the application review, and the agency's definitions, the Service determined that transferring information and materials to the data subject required searching, analyzing, and processing information from various territorial units of the agency. Due to the need to ensure the smooth implementation of social work for other minors (related beneficiaries of the agency), the agency proportionally limited the data subject's right by extending the timeframe beyond the period established by law. The data subject could reasonably anticipate the delay in receiving the requested information, as the data controller promptly communicated the need to search for information. Considering the legal basis for the agency's proportional limitation of the data subject's right and the necessity behind it, there was no indication of the agency committing an administrative offense in relation to informing the data subject.

The decision of the Service highlighted that while the agency informed the applicant about the need to gather information from various units, the correspondence did not clearly articulate that the information couldn't be provided within the legally mandated timeframes or specify when it would be available. In its ruling, the Service invoked Article 3 of the UN Convention “on the Rights of the Child”, emphasizing that all actions concerning children, whether conducted by state or private entities in the social welfare sector, courts, administrative bodies, or legislative bodies, must prioritize the best interests of the child. The Service underscored that the exercise of the right to request information/documentation by the data subject typically corresponds to the timely exercise of one's rights in various legal proceedings, with particular importance placed on protecting the rights of minors. Consequently, according to the decision of the President of the Service, the agency was directed to provide the data subject with clear information regarding the purpose and duration of any restriction on the right in cases where there are objective grounds for such restriction.

❖ *LEPL - Agency for State Care and Assistance for the Victims of Human Trafficking*

The Personal Data Protection Service, prompted by a minor with disabilities under state care, conducted an examination regarding the lawfulness of information dissemination by the LEPL - Agency for State Care and Assistance for Victims of Human Trafficking (hereafter referred to as "the Agency").

During the examination, it was found that on December 13, 2022, the minor submitted a request to the agency for documentation containing his personal data. This request was initially written in Braille and later transcribed by the minor's school teacher. The agency responded, explaining that due to the extensive nature of the requested documentation, which amounted to up to 200 pages, it lacked the resources to process such a large volume of documents and provide them in Braille format to the applicant. As part of their assessment of how to transfer the documentation to the minor, the agency reached out to the director of the minor's school. The school expressed readiness to receive the documentation and present it to the minor. However, the agency deemed it inappropriate to provide the requested documentation to the school, as it was considered a third party and not the minor's official representative. Additionally, the sensitive information contained in the case file factored into this decision.

Based on the agency's explanation, the minor provided the official address of an organization in their statement. However, at the time of the application submission, the employees of the organization did not possess the appropriate power of attorney, which would authorize them to receive or obtain materials containing the minor's personal data. Based on the provided information, the agency deemed it inappropriate to send the documents containing the minor's data to the organization's lawyers before they were granted proper authority. Additionally, the agency indicated that in December 2022, the minor was assigned a social worker who went on sick leave. As of January 1, 2023, the employment relationship between the said social worker and the agency was terminated. Subsequently, the minor was assigned a new social worker. Considering the agency's human resources and the volume of requested material, the social worker was unable to provide the relevant documents to the minor, and thus the minor's application of December 13, 2022, could not be fulfilled.

The lawyers representing the organization defending the rights of minors, in a statement submitted to the agency on January 27, 2023, requested that the agency grant them representative authority to protect the rights of minors. Consequently, on February 6, 2023, the agency issued a power of attorney, and on the same day, the lawyer from the same organization was handed over the complete documentation containing the minor's personal data.

It's significant to note that as part of the criminal case investigation concerning violence against the minor, the Prosecutor's Office of Georgia requested the materials related to the minor from the Agency. The Agency complied with this request by sending the complete material containing the minor's data on December 29, 2022.

As a result of examining the issue, the Personal Data Protection Service (hereinafter - the Service) noted in its decision that, based on the data processing standards established by law, the right of the data subject to apply to the data controller and request documentation containing their data is a crucial prerequisite for realizing the data subject's rights. This right empowers the data subject to review documents containing their data, obtain copies, and understand the context and manner in which their data is being processed. This opportunity grants the data subject insight into the lawful processing of their data and aids in defining and safeguarding their interests. It stressed that the effective exercise of this right is especially vital in cases concerning the legal interests of a child with disabilities. Ensuring the child or their chosen representatives are equipped with pertinent information is crucial, particularly for their active and informed participation in various legal proceedings. In relation to this, the Service referred to the first, second, and third parts of Article 5 of the "The Code on the Rights of the Child," which state that the child has the right to have their best interests prioritized. These best interests are defined individually for each child in accordance with this Code, the Constitution of Georgia, the Convention on the Rights of the Child, its additional protocols, and other international treaties of Georgia. The Service emphasized that when determining the best interests of the child, factors such as the child's right to personal development within a family environment, their social and cultural background, their capacity to exercise rights independently, and their opinions must be considered. Moreover, prioritizing the child's best interests is obligatory for legislative, executive, and judicial bodies of Georgia, as well as for public institutions, individuals, and legal entities when making decisions or taking actions concerning the child.

The decision also cited Article 8, subparagraph “b” of the Council of Europe Convention of January 28, 1981 for the “Protection of Individuals with regard to Automatic Processing of Personal Data”. This article states that any individual should have the ability, if necessary, to periodically and without excessive delay or expense, confirm the existence of personal data related to them in an automated file, as well as receive this data in an acceptable form. Furthermore, the right of the data subject to request materials containing their data and the extent to which the request is fulfilled is regulated by Article 21, Paragraph 5 of the Law of Georgia "On Personal Data Protection". According to this article, a person has the right to access and obtain copies of their personal data held by a public institution.

Based on the legal and factual circumstances presented, the Service did not find the agency's reasoning for the delay in satisfying the minor's application to be valid. The decision mentions that the period from December 13, 2022, to February 6, 2023, which the agency used to satisfy the applicant's request, is not reasonable. This is evidenced by the fact that the requested documentation was found and transferred to the Prosecutor's Office of Georgia on December 29, 2022, within a much shorter timeframe. Therefore, the extended period is inconsistent with the best interests of the minor. As a result, the LEPL - Agency for State Care and Assistance for the Victims of Human Trafficking was found to have violated an administrative offense outlined in the first paragraph of Article 50 of the Law of Georgia "On Personal Data Protection" and was issued a warning as an administrative fine.

5. International Legal Instruments and Practices for Processing Minors' Data

5.1. Protection of the Right to Privacy of Minors in the Legal System of the United Nations

Article 12 of the Universal Declaration of Human Rights ("UDHR")[311] acknowledged, for the first time at the international level, the right to respect for an individual's personal and family life, prohibiting unreasonable interference in a person's personal space. This declaration is considered foundational in the development of international human rights law.[312] Similarly, Article 17 of the International Covenant on Civil and Political Rights reaffirms this principle, emphasizing the prohibition of arbitrary and unlawful interference in personal space, residence, or correspondence.[313]

The 1989 Convention on the Rights of the Child ("CRC")[314] sets forth minimum standards for safeguarding the welfare of minors, recognizing the necessity for special care and protection

[311] United Nations (UN), Universal Declaration of Human Rights, 10 December, 1948.
[312] Handbook on European Data Protection Law, 2018 edition, 21.
[313] United Nations (UN), International Covenant on Civil and Political Rights, 16 December 1966.
[314] UN, Convention on the Rights of the Child, Adopted and opened for signature, ratification and accession by General Assembly resolution 44/25 of 20 November 1989.

of children.[315] This convention, ratified by the largest number of countries in history,[316] has prompted states to revise legal frameworks concerning children.[317] Notably, member states of the Council of Europe and the European Union are parties to this convention, underscoring its significance across Europe. The convention imposes obligations on states and relevant institutions to ensure the protection of children's rights.[318]
The main principles of the Convention entail:

- *Prohibition of discrimination*: Ensuring the rights of the child without any form of discrimination;
- *Best interests of the child*: The best interests of the child must be paramount in any decision or action affecting them;
- *The right to life and development of the child*: Every child deserves the opportunity to develop comprehensively—physically, mentally, spiritually, morally, socially, and otherwise;
- *Respecting the child's opinions*: Children should be afforded the chance to express their views on matters concerning them and participate in decisions regarding their lives, considering their age and developmental stage;[319]

Within the framework of the 1989 Convention on the Rights of the Child, Article 16 guarantees the protection of children's personal data, stating that: "*No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation.*" It's important to consider that at the time of the Convention's adoption in 1989, modern technologies were not as advanced

[315] Children's rights in the digital environment: Moving from theory to practice, Best practice guideline, May 2021, 4, <https://www.betterinternetforkids.eu/documents/167024/200055/Best-practice+guideline+-+Childrens+rights+in+the+digital+environment+-+May+2021+-+v2+FINAL+CC+BY.pdf/f947d4f9-4ec4-49ae-5e2e-b6e9402c5fa2?t=1624532196598>, [11.08.2023].

[316] Unicef, Convention on the Rights of the Child, https://www.unicef.org/child-rights-convention#:~:text=In%201989%2C%20world%20leaders%20made,children's%20lives%20around%20the%20world, [11.08.2023].

[317] Unicef, for every child, Convention on the Rights of the Child for every child, every right, <https://www.unicef.org/child-rights-convention#:~:text=In%201989%2C%20world%20leaders%20made,children's%20lives%20around%20the%20world>, [15.08.2023].

[318] Handbook on European Law relating to the rights of the child, 2017, 27.

[319] Information Commissioner's Office (ICO), The United Nations Convention on the rights of the child and what it means for online services, <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/how-to-use-our-guidance-for-standard-one-best-interests-of-the-child/the-united-nations-convention-on-the-rights-of-the-child/#:~:text=The%20UNCRC%20embodies%20the%20idea,been%20transformed%20in%20many%20areas>, [15.08.2023].

as they are today, and thus, children did not have active access to the Internet. Consequently, the original legal framework regarding rights was not tailored to today's digital reality, resulting in a lower risk of personal data breaches. However, it's noteworthy that a separate provision of the Convention allows for interpretation to ensure the proper protection of children's rights, including within the digital realm.[320]

In early 2018, the Committee on the Rights of the Child embarked on developing a general comment addressing the relevance of the Convention to the digital world. This comment came into effect on March 24, 2021, outlining how states should act to uphold children's rights in the digital sphere.[321] Given the ever-evolving nature of the digital realm, ensuring adequate safeguards for children's rights is of paramount importance.[322] To achieve this, member states of the convention must enact national legislation aligned with international standards.[323]

5.2. Council of Europe Legal Framework on the Protection of Personal Data of Minors

Within the Council of Europe framework, the right to protect personal data is enshrined in Article 8 of the "Convention for the Protection of Human Rights and Fundamental Freedoms",[324] which guarantees the right to privacy, family life, home, and correspondence, while delineating conditions for limiting these rights. Paragraph 2 of Article 8 sets forth three criteria for evaluating the legitimacy of governmental restrictions on these rights: a) compliance with the law; b) lawful purpose; c) necessity in a democratic society. Matters concerning the alleged infringement of children's personal data also fall within the purview of Article 8 of the Convention. Consequently, the European Court of Human Rights adjudicates on claims of children's personal data violations in accordance with the stipulations outlined in the aforementioned article.

It's worth highlighting that the 1981 Council of Europe “Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data” (Convention 108), along with its Additional Protocol, represents the first legally binding international instrument in this domain. Convention 108 and its Additional Protocol pertain to data processing across both

[320] Children’s rights in the digital environment: Moving from theory to practice, Best practice guideline, May 2021, 4-5.
[321] UN Committee on the Rights of the Child, ‘General Comment No. 25 (2021) on Children’s Rights in Relation to the Digital Environment, 3.
[322] Ibid., 1.
[323] Ibid., 4.
[324] CoE, European Convention for the Protection of Human Rights and Fundamental Freedoms, 1950.

private and public sectors, aiming to safeguard individuals during the processing of personal data, thereby mitigating potential infringements on their rights.[325] The principles outlined in Convention 108 pertain to the fair and lawful collection and processing of personal data, which should be conducted for the initially designated legitimate purposes. Furthermore, data retention should be limited to the necessary duration. Additionally, without adequate legal safeguards, the processing of "special category" personal data is prohibited. The Convention upholds the right of individuals, including children, to be informed about the information stored about them and, where necessary, to rectify such information.[326]

5.2.1. Overview of the practice of the European Court of Human Rights

The European Court of Human Rights (ECtHR) has extensively deliberated on safeguarding the rights of children and upholding privacy rights in various rulings. Notably, the ECtHR frequently invokes the UN Convention on the Rights of the Child and draws upon the principles enshrined in the 1989 Convention on the Rights of the Child in its legal deliberations. Precedent set by the European Court underscores states' obligation to enact effective measures to safeguard children's right to privacy. This chapter delves into several pivotal rulings of the European Court, shedding light on the court's stance on the protection of children's personal data.

In the case "*K.U. v. Finland*,"[327] the applicant was a child who complained about a sexually explicit statement posted in his name on a dating website. The Service provider declined to reveal the identity of the individual responsible for posting the information, citing confidentiality obligations mandated by Finnish law. As per the complainant's argument, national legislation lacked adequate safeguards for protecting their rights. The European Court of Human Rights has ruled that states bear a positive obligation to implement suitable measures to uphold the right to privacy, even within interpersonal relationships. In this instance, the state should have undertaken effective measures to identify and prosecute the individual responsible for the wrongdoing. By failing to fulfill this obligation, the court concluded that there was a violation of Article 8 of the “Convention for the Protection of Human Rights and Fundamental Freedoms”.[328]

---

[325] Handbook on European Law relating to the rights of the child, The Council of Europe (CoE) and the European Court of Human Rights (ECtHR), 2015, 193.
[326] Ibid.
[327] ECtHR, K.U. v. FINLAND, Appl. No. 2872/02, 2 December 2008, <https://hudoc.echr.coe.int/?i=001-89964>, [16.08.2023].
[328] Handbook on European Law relating to the rights of the child, The Council of Europe (CoE) and the European Court of Human Rights (ECtHR), 2015, 191.

The case "*Avilkina and Others v. Russia*"[329] revolves around the disclosure of medical records belonging to a two-year-old girl, prompted by a prosecutor's inquiry. The purpose of the request was to obtain information about the refusal of Jehovah's Witnesses to receive blood transfusions. The court observed that the public interest in probing a crime might supersede both the patient's and the public's interest in maintaining medical record confidentiality. Furthermore, it was highlighted that the applicant neither represented the accused nor the suspect in the criminal proceedings. The medical personnel treating the applicant had the option to seek court authorization to administer a blood transfusion if they deemed it essential to save the patient's life. Given the absence of a compelling societal necessity for divulging information pertaining to the applicant's health, the European Court concluded that there was a violation of Article 8 of the "Convention for the Protection of Human Rights and Fundamental Freedoms".[330]

In the case of "*S. and Marper v. the United Kingdom*,"[331] investigative authorities obtained fingerprints and DNA samples from an eleven-year-old child, even though the statute of limitations had expired for the charge of attempted robbery. The retention of such personal information, considering its nature and extent, constituted an infringement upon the first applicant's right to privacy. The prevailing principles within the Council of Europe and the legislation of other member states, as well as established practices, mandate that member states maintain personal data in proportion to the purpose of its processing. Furthermore, it is imperative to limit data retention to the shortest feasible duration, a principle especially pertinent within the law enforcement system. The court found the indefinite storage period for data, irrespective of the legal nature and severity of the offense, concerning. Particularly for minors, the storage of personal data could be significantly detrimental, contingent upon their integration and societal development context. Consequently, the court concluded that the storage of data constituted a disproportionate intrusion into the applicant's protected sphere of privacy, thereby establishing a violation of Article 8 of the "Convention on the Protection of Human Rights and Fundamental Freedoms".[332]

[329] Avilkina and Others V. Russia, Appl. No. 1585/09, 6 June 2013, <https://hudoc.echr.coe.int/eng?i=001-120071>, [17.08.2023].
[330] Handbook on European Law relating to the rights of the child, The Council of Europe (CoE) and the European Court of Human Rights (ECtHR), 2015, 192.
[331] ECtHR, S. and Marper v. the United Kindgom [GC], Nos. 30562/04 and 30566/04, 4 December 2008, <https://hudoc.echr.coe.int/eng?i=001-61194>, [17.08.2023].
[332] Handbook on European Law relating to the rights of the child, The Council of Europe (CoE) and the European Court of Human Rights (ECtHR), 2015, 192.

5.2.2. Documents Developed by the Committee of Ministers of the Council of Europe

In 2018, the Committee of Ministers of the Council of Europe formulated a recommendation outlining the fundamental principles for respecting and safeguarding children's rights in the digital sphere. Although non-binding, this recommendation draws upon the legally binding conventions of the Council of Europe and incorporates standards and recommendations from the United Nations regarding children's rights. The guidelines underscore the significance of states prioritizing the protection and preservation of a child's privacy and personal data. Additionally, the recommendation delineates key principles pertaining to the protection of children's personal data, notably: prioritizing the best interests of the child; nurturing the child's developmental capacities; prohibiting discrimination; considering children's perspectives; and involving all relevant stakeholders in decisions concerning children. Furthermore, it enumerates a roster of children's rights that warrant particular attention in the era of modern technologies, including: access to the digital realm; freedom of expression and access to information; the right to engage in participation, recreation, assembly, and association; privacy and data protection; access to education; entitlement to protection and security; and access to legal remedies when necessary.[333]

In 2019, the Committee of Ministers issued a recommendation to member states concerning the advancement of digital citizenship education. This recommendation underscored the significance of imparting digital citizenship education to children, emphasizing the importance of fostering their digital literacy and responsibility. Furthermore, it emphasized the role of parents and legal guardians in promoting children's engagement in the digital sphere while maintaining a balanced approach to online safety and participation. 8itionally, the recommendation highlighted the crucial role of educators in this domain.[334]

On April 28, 2021, the Committee of Ministers of the Council of Europe ratified the Declaration titled "On the Need to Protect the Privacy of Children in the Digital Environment," aimed at bolstering the fulfillment of rights outlined in the UN Convention on the Rights of the Child and the European Convention for the Protection of Human Rights and Fundamental Freedoms. This declaration highlights the risks encountered by children in their utilization of modern technologies. Moreover, it stresses the criticality of bolstering the

[333] Recommendation CM/Rec (2018)7 of the Committee of Ministers, Guidelines to respect, protect and fulfil the rights of the child in the digital environment, 4 July 2018, <https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016808b79f7>, [18.08.2023].

[334] Recommendation CM/Rec(2019)10 of the Committee of Ministers to member States on developing and promoting digital citizenship education, <https://library.parenthelp.eu/wp-content/uploads/2019/12/CoE-digital-citizenship-education-recommendations-CM_Rec201910E.pdf>, [22.08.2023].

protection of children's privacy and personal data, especially amidst the challenges posed by the COVID-19 pandemic.[335]

In addition to the aforementioned initiatives, the Council of Europe has crafted a strategy document for 2022-2027, which underscores various issues concerning children, with a particular emphasis on their engagement with modern technologies. This document delineates six primary priority areas, one of which is ensuring universal access to technology for all children and promoting their safe utilization of such resources. Furthermore, it acknowledges that the shift to online education during the COVID-19 pandemic has introduced a host of challenges regarding the protection of children's personal data.[336]

5.3. Regulation Of Personal Data Protection Of Minors In The European Union

In Europe, privacy and data protection rights are considered fundamental to democracy. Article 7 of the "Charter of Fundamental Rights of the European Union"[337] ensures respect for private and family life, and Article 8 establishes the right to data protection and defines it as a fundamental right. The first paragraph of the latter article ensures the right to data protection, its second paragraph establishes the essential principles of data protection, and the third paragraph emphasizes that the implementation of these principles should be ensured by an independent supervisory body.[338]

On May 25, 2018, the EU General Data Protection Regulation ("GDPR")[339] came into effect, establishing a new global benchmark in personal data protection. The regulation aims to effectively safeguard individuals' rights amidst technological advancements and contemporary challenges. Notably, the GDPR places significant emphasis on the protection of children's personal data. Paragraph 38 of the preamble underscores the necessity for special safeguards when processing children's personal data, recognizing that children may have limited awareness of the risks, consequences, remedies, and rights associated with such processing.[340] Furthermore, when informing children about these risks, their age, level of development, and

[335] Declaration by the Committee of Ministers on the need to protect children's privacy in the digital environment, 28 April 2021, <https://search.coe.int/cm/pages/result_details.aspx?ObjectId=0900001680a2436a>, [23.08.2023].
[336] Council of Europe Strategy for the Rights of the Child (2022-2027), "Children's Rights in Action: from continuous implementation to joint innovation".
[337] Charter of Fundamental Rights of the European Union, 2000/C364/01.
[338] Handbook on European Data Protection Law, 2018, 28.
[339] 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 (General Data Protection Regulation).
[340] Ibid., recital 38.

skills should be considered, as these factors influence their capacity to mitigate risks effectively.[341]

The Court of Justice of the European Union ("CJEU") draws upon fundamental principles strengthened by the 1989 Convention "on the Rights of the Child".[342] It is noteworthy that the Court exercises particular diligence in addressing matters concerning children.

In March 2021, two significant documents were released concerning the European Union's initiatives for safeguarding and advancing children's rights in the digital realm.[343] The first document pertains to the European Union's strategy[344] regarding children's rights, serving as a framework for action for both the European Commission and member states. It delineates six thematic areas and outlines key activities planned by the European Commission to enhance the protection of children's rights. According to the strategy document, the pandemic has exacerbated challenges that children encounter in the online sphere daily, including frequent occurrences of cyberbullying, exploitation, and the dissemination of sexual content materials. The strategy document is based on the Convention on the Rights of the Child and the Council of Europe standards regarding child rights protection.[345] The second document, the "Digital Compass,"[346] crafted by the European Commission, amalgamates the vision, objectives, and perspectives for Europe's successful digital transformation by 2030. The European Commission emphasizes the imperative of actualizing the digital rights of children within this framework.[347]

5.4. Approaches and Practices of Foreign Personal Data Protection Supervisory Authorities

Data Protection Authorities ("DPAs")[348] place particular emphasis on safeguarding children's personal data. The growing adoption of modern technologies by children amplifies the risks associated with protecting their right to privacy. Illicit processing of minors' personal data can

[341] Data Protection Commission (DPC), The Fundamentals for a Child-Oriented Approach to Data Processing, 12.
[342] CJEU, C-244/06, Dynamic Medien Vertriebs GmbH v. Avides Media AG, 14 February 2008, paras. 42 and 52.
[343] Children's rights in the digital environment: Moving from theory to practice, Best-practice guideline, 2021, 6.
[344] European Commission, "EU Strategy on the Rights of the Child" <https://ec.europa.eu/info/sites/default/files/child_rights_strategy_version_with_visuals3.pdf>, [24.08.2023].
[345] Children's rights in the digital environment: Moving from theory to practice, Best-practice guideline, 2021, 6-7.
[346] Europe's Digital Decade: Commission sets the course towards a digitally empowered Europe by 2030, <https://ec.europa.eu/commission/presscorner/detail/en/IP_21_983>, [25.08.2023].
[347] Children's rights in the digital environment: Moving from theory to practice, Best-practice guideline, 2021, 7.
[348] Data Protection Authorities.

inflict irreparable harm on their psychological well-being. Therefore, alongside the advancement of legal safeguards, raising public awareness is paramount.

The United Kingdom's Data Protection Supervisory Authority ("ICO")[349] has formulated guidance concerning the protection of children's personal data.[350] This document is designed for organizations engaged in processing children's personal information. Notably, in alignment with the Convention on the Rights of the Child, a child is defined as an individual under the age of 18. The United Kingdom's General Data Protection Regulation — "UK GDPR" incorporates provisions aimed at bolstering the safeguarding of children's personal data and facilitating the dissemination of information in clear and comprehensible language. Ensuring transparency and accountability in children's usage of online services is imperative.[351] In addition to the aforementioned initiatives, the ICO has developed a privacy training course tailored for teachers. This course aims to educate teachers about personal data protection and empower them to disseminate this knowledge to children. The materials are readily accessible and open for anyone to utilize.[352] Moreover, the ICO has introduced the "Design Test",[353] aimed at assisting designers in ensuring compliance with the Children's Code for various products and services that children are likely to access. The objective of the "Age Appropriate Design: Code of Practice for Online Services"[354] is to facilitate GDPR compliance, thereby integrating appropriate safeguards for protecting children's personal data within digital services. Each test[355] includes comprehensive information outlining best practices and measures necessary to adhere to the Children's Code.

The Data Protection Supervisory Authority of Ireland ("DPC")[356] has released a guide titled "The Fundamentals for a Child-Oriented Approach to Data Processing."[357] This document aims to elevate standards for the processing of children's data by presenting fundamental principles

---

[349] Information Commissioner's Office (ICO).

[350] Information Commissioner's Office (ICO), Children and the GDPR, 22 March 2018.

[351] Ibid., 8.

[352] Information Commissioner's Office (ICO), New school resources for teachers, <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/school-resources>, [29.08.2023].

[353] IAPP, ICO creates Children's Code design tests, <https://iapp.org/news/a/uk-ico-creates-childrens-code-design-tests>, [29.08.2023].

[354] Explanatory memorandum to the Age Appropriate Design Code 2020, <https://www.gov.uk/government/publications/explanatory-memorandum-to-the-age-appropriate-design-code-2020-2020/explanatory-memorandum-to-the-age-appropriate-design-code-2020-2020>, [29.08.2023].

[355] ICO, Information Commissioner's Office (ICO), Children's Code design tests, <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/designing-products-that-protect-privacy/childrens-code-design-guidance/practical-tools/childrens-code-design-tests/>, [29.08.2023].

[356] Data Protection Commission (DPC).

[357] Data Protection Commission, Fundamentals for a Child-Oriented Approach to Data Processing, 2021.

and pertinent measures to safeguard children's rights in both digital and offline contexts. By delineating these principles, the guide assists controllers in fulfilling their obligations outlined in the GDPR. Similar to the ICO, the Irish supervisory authority aligns its definitions with those outlined in the UN Convention on the Rights of the Child. The DPC has delineated key aspects to be considered when processing children's personal data, such as: ensuring a high level of data protection; obtaining explicit consent; defining the target audience; providing detailed information; prioritizing child-centered transparency; and taking into account children's opinions, among others.[358]

On June 22, 2023, the Spanish Data Protection Supervisory Authority ("AEPD")[359] declared its endorsement for the proposal of a state agreement concerning the protection of children's personal data while utilizing the Internet and social media platforms. This initiative concentrates on addressing the risks minors encounter when engaging with pertinent online services. From this perspective, the AEPD underscored that backing this initiative ensures the effective safeguarding of children's personal data.[360]

The French Data Protection Supervisory Authority ("CNIL")[361] has undertaken numerous initiatives to safeguard children's personal data.[362] Among these efforts, CNIL has issued eight recommendations aimed at protecting children's personal data in the digital sphere.[363]These recommendations were developed through comprehensive examination of the issues surrounding children's personal data protection, including relevant challenges. It is noteworthy that these recommendations were crafted following public consultations and thorough legal analysis. Additionally, CNIL has organized workshops involving children to gain insights into their perceptions of privacy and data protection.[364] The objective behind developing these recommendations is to offer practical guidance and clear explanations regarding legislative provisions. These recommendations are intended for children, parents, and individuals working within the digital realm.

[358] Ibid., 6.
[359] Spanish Agency for Data Protection (AEPD).
[360] OneTrust DataGuidance, Spain: AEPD supports initiative on minors' protection in digital environment, 2023, <https://www.dataguidance.com/news/spain-aepd-supports-initiative-minors-protection>, [29.08.2023].
[361] Commission Nationale de l'Informatique et des Libertés (CNIL).
[362] CNIL, Digital rights of children, <https://www.cnil.fr/en/digital-rights-children>, [29.08.2023].
[363] CNIL, 8 recommendations to enhance the protection of children online, 09 August 2021,<https://www.cnil.fr/en/cnil-publishes-8-recommendations-enhance-protection-children-online>, [30.08.2023].
[364] Ibid.

The Swedish Data Protection Supervisory Authority ("IMY")[365] is actively engaged in safeguarding children's personal data. In collaboration with other agencies, IMY has devised guidelines[366] aimed at bolstering the protection of children's rights, aligning with the principles of the GDPR and the Convention on the Rights of the Child. These guidelines offer practical tips for safeguarding children's personal data in the digital realm. The overarching goal of these recommendations is to ensure effective protection for children when navigating modern technologies.[367]

Indeed, data protection supervisory bodies have extensively deliberated on the protection of children's personal data. While only a few decisions of these authorities are presented here for illustrative purposes, they provide a broad overview of the prevailing approaches concerning the safeguarding of children's personal data.

The United Kingdom's Data Protection Supervisory Authority ("ICO") conducted an investigation into the lawfulness of processing children's data on the Internet platform "TikTok," which occurred without parental consent. In accordance with the United Kingdom's General Data Protection Regulation ("UK GDPR"), controllers are required to obtain consent from parents or legal representatives when providing certain services to individuals under the age of 13. The supervisory authority highlighted the potential risks associated with the use of children's data for "tracking" and "profiling," which could be detrimental to children. Conversely, children accessing the platform might be exposed to unwanted content during their browsing experience. TikTok enabled over a million children under the age of 13 in the UK to access its platform. According to the supervisory body, TikTok utilized personal data associated with children without parental consent and lacked adequate age verification mechanisms. Moreover, there was no provision for removing users under 13 from the platform. Additionally, TikTok fell short in providing comprehensive information to users regarding the collection and processing of their data. As a result of these shortcomings, TikTok was fined for its failure to ensure legal, fair, and transparent processing of personal data.[368]

It's worth noting that the Dutch Data Protection Supervisory Authority[369] also scrutinized the Internet platform TikTok. The supervisory authority highlighted that a significant number of

[365] Swedish Authority for Privacy Protection (IMY).
[366] The rights of Children and Young People on Digital Platforms, Stakeholder Guide, Swedish Authority for Privacy Protection.
[367] Ibid., 3.
[368] Information Commissioner's Office (ICO), GDPRhub, <https://gdprhub.eu/index.php?title=ICO_(UK)_-_TikTok_ICO>, [30.08.2023].
[369] Dutch Data Protection Authority (AP).

children under the age of 16 in the Netherlands utilize the platform. During the account creation process, users are presented with the privacy policy in Dutch and are required to consent to it. However, the supervisory authority discovered that between May 25, 2018, and July 28, 2020, Dutch users, including children, were only provided with information about the privacy policy in English. As a result of this oversight, TikTok violated the first paragraph of Article 12 of the GDPR, which stipulates that data controllers must take appropriate measures to furnish data subjects with information in a concise, transparent, intelligible, and easily accessible format, using clear and plain language, particularly when the subject is a minor. Taking into account the circumstances, the Dutch supervisory authority levied a fine against the TikTok platform.[370]

The Spanish data protection supervisory authority has indeed investigated instances of unlawful processing of children's personal data. In one particular case, a gymnastics club published a photograph of two children during training on its Instagram page. The mother of the minors repeatedly requested the club to refrain from publishing photos of her children on social networks. Additionally, she clarified that she had not given consent for the gymnastics club to photograph or record her 10- and 12-year-old daughters. As a result of the complaint filed by the mother, the Spanish data protection supervisory authority determined that the club violated the first paragraph of Article 6 of the GDPR by publishing pictures of the applicant's children on Instagram without a legal basis. The club failed to demonstrate that it had the right to process the data of the applicant's minor children. Consequently, the Spanish Data Protection Supervisory Authority imposed a fine of 5,000 euros on the gymnastics club.[371]

Indeed, the decision made by the Irish Data Protection Supervisory Authority concerning the processing of personal data by the platform Instagram is noteworthy in terms of safeguarding children's personal data. The authority prohibited the processing of personal data of minor users, specifically the public disclosure of children's email addresses, telephone numbers, and the automatic disclosure of personal accounts on Instagram. It was revealed that Instagram permitted users aged between 13 and 17 to operate business accounts on the platform. Users' phone numbers and email addresses were indeed publicly visible on the accounts, and the platform had a user registration system that automatically made accounts of users aged 13 to 17 public. After conducting a thorough investigation, the Irish supervisory authority imposed a fine of 405 million euros on the organization. This included a specific fine of 20 million euros for the violation of the first paragraph of Article 6 of the GDPR. Additionally, the Irish

[370] AP (The Netherlands) – TikTok, GDPRhub, <https://gdprhub.eu/index.php?title=AP_(The_Netherlands)_-_TikTok>, [30.08.2023].

[371] GDPR hub, AEPD (Spain) - PS/00209/2021, <https://gdprhub.eu/index.php?title=AEPD_(Spain)_-_PS/00209/2021>, [30.08.2023].

supervisory authority mandated Instagram to implement various measures to ensure that its processing operations align with the requirements of the GDPR.[372]

5.5. Global Privacy Assembly ("GPA") Resolution on the Digital Rights of the Child

In 2021, the Global Privacy Assembly ("GPA") adopted Resolution on digital rights,[373]emphasizing the necessity for heightened protection of children. According to the resolution, children are entitled to the rights enshrined in the UN Convention on the Rights of the Child, which should be applicable across all aspects of life, including the digital sphere. The resolution underscores the significant impact of the digital environment on children's development, daily activities, future prospects, and opportunities.[374] Indeed, every action conducted in the online realm leaves a digital footprint, and once information is uploaded onto the internet, control over it may be lost. Posted information may be collected and utilized without the specific knowledge of third parties. A recommendation has been put forth to service providers, emphasizing the importance of fostering an understanding of responsibility among children when utilizing online services.[375]

[372] Data Protection Commission, Data Protection Commission announces decision in Instagram Inquiry, <https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-instagram-inquiry>, [30.08.2023].
[373] Global Privacy Assembly (GPA) 43rd Closed Session of the Global Privacy Assembly October 2021 Adopted Resolution on children's digital rights.
[374] Ibid.
[375] Ibid.

Address: 7, Vachnadze Str. 0105, Tbilisi, Georgia
48, Baku Str. 6010, Batumi, Georgia
www.personaldata.ge
Tel.: (+995 32) 242 1000
E-mail: office@pdps.ge