Tamar Samniashvili*

Data Subject Consent as a Legal Basis: Theoretical and Practical Perspectives

The article discusses the data subject consent institution as a legal basis for the processing of personal data. It analyzes the criteria of lawful consent, including voluntariness, active expression of will, specificity, and clarity. The particular importance of consent in the processing of children's personal data and special category data is emphasized. The study examines the peculiarities of consent formulation in documents, contracts, and online environments, emphasizing the mandatory protection of transparency and informed consent principles.

The article is based on a comparative analysis of Georgian national legislation and international law, particularly the European Union's General Data Protection Regulation (GDPR).[1] Key challenges and risks in the practical implementation of the consent institution are identified.

The article presents the criteria necessary for the effective functioning of consent, whose implementation in practice contributes to the development of a data protection culture and the strengthening of public trust in both private and public sectors.

Keywords: *personal data, special category data, personal data of a child, consent, child's consent, right to withdraw consent, consent in a contract, consent in the online environment, pre-existing records ("cookie files"), General Data Protection Regulation (GDPR)*

* Master of Law, Ilia State University; Data Protection Officer at the LEPL – National Archives of Georgia.

[1] 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 (შემდგომში — GDPR)

1. Introduction

The consent of the data subject as a legal basis for the processing of personal data is provided for by the Law of Georgia on Personal Data Protection.[2] The issue that a data controller requires a legal basis for processing personal data is not new. Alongside the growing legal awareness of society, there is an increase, on the one hand, in the expectations and demands of data subjects, and on the other hand, in the obligations of data controllers to process data in accordance with the law.

Consent, as a legal basis for the processing of personal data, represents one of the most frequently used and relevant issues in practice. However, the Swedish Authority for Privacy Protection notes, when discussing the issue of consent, that: "consent is normally not the easiest nor the most appropriate alternative, for example because the person who gives their consent can revoke it at any time."[3]

In most cases, data controllers use this basis to bring existing or planned processes into compliance with the law. Specifically, in cases where no other legal basis for processing exists, the data controller establishes a legal basis for the process by obtaining consent. In such cases, there is a risk that consent may become a "universal instrument" allowing controllers to merely formalize processes within a legal framework. Accordingly, the risks associated with obtaining and subsequently implementing this legal basis should not be overlooked.

The Information Commissioner's Office (ICO) provides guidance on consent, according to which, for a specific processing activity, the lawful basis that most accurately reflects the purpose of the processing and the actual relationship with the data subject should be chosen."If consent is difficult, this is often because another lawful basis is more appropriate, so you should consider the alternatives".[4]

The importance of consent becomes even more apparent in the modern digital reality. In the era of Internet services, social networks, mobile applications, and digital marketing, the vast majority of data processing is based precisely on consent. Users press the "I agree" buttons daily, yet in reality, they rarely have the time or opportunity to fully understand what this consent entails and how genuinely free their choice is. Therefore, in recent years, discussions about the problem of "formal consent" and its effectiveness have intensified.

The use of consent in practice is particularly relevant in the private sector, where it is often associated with direct marketing, employment processes, insurance and banking services, and data processing in the education and healthcare sectors. In the public sector, the use of consent is comparatively limited, since data processing in these cases is mostly based on legally established obligations or public interest. In such

[2] Law of Georgia on Personal Data Protection 14/06/2023, Article 5(1)(a).

[3] *Swedish Authority for Privacy Protection*, The rights of children and young people on digital platforms, Stakeholder guide, 15, <https://www.imy.se/globalassets/dokument/rapporter/the-rights-of-children-and-young-people-on-digital-platforms_accessible.pdf> [27.11.2025].

[4] *Information Commissioner's Office (ICO)* Guideline on *When is consent appropriate?* <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/consent/when-is-consent-appropriate/> [27.11.2025].

cases, the issue of voluntariness is particularly sensitive, as citizens often cannot perceive consent as a free choice in their interactions with public institutions. Therefore, in most cases, public authorities cannot rely on the consent of the data subject, considering the balance of power between the data subject and the data controller.[5]

The aim of the article is not only to provide a theoretical analysis of consent as a legal basis for data processing but also to highlight its practical significance, associated risks, and development perspectives.

2. Processing of Personal Data on the Basis of Consent

The Law of Georgia on Personal Data Protection defines the concept of consent and specifies the mandatory criteria for considering this legal basis as lawful:[6]

- **After receiving information** – consent must not be given in advance; it must be provided after the data subject has been informed about the matter for which consent is requested. This ensures, in turn, the possibility of a genuine choice.
- **Informed** – data controllers must ensure that clear and simple language is used for information purposes. The text must be easily understandable to any individual, not only to legal professionals, and must not include long, complex privacy policies or rules presented exclusively in legal terminology. The consent request must be distinct from other matters and communicated in plain, comprehensible language.
- **Specific purpose** – this criterion is directly linked to the requirement for adequate information. The data subject must be aware of the precise purpose for which their personal data is being processed and what they are consenting to.
- **Active engagement** – consent must be actively expressed by the data subject. In practice, this may take the form of marking a consent box in the presence of a written document, providing consent via a hyperlink, giving verbal consent, or another appropriate method.
- **Freely given** – consent must be voluntary, meaning the data subject must be able to make a decision regarding the processing of their personal data independently and without any pressure.
- **Unambiguous** – the data subject's intent regarding specific data and its specific processing must be clear and must not give rise to doubt regarding its existence.

[5] Guideline Recommendation of the Personal Data Protection Service of Georgia on "Obtaining Consent from the Data Subject", 10.
[6] Law of Georgia on Personal Data Protection 14/06/2023, Article 3(m).

- **Form** – consent may be provided in writing (including electronically) or verbally, depending primarily on the category of data for which consent is given. Specifically, for special categories of data, consent can only be given in written form.[7] The Law also provides similar specific regulation for direct marketing when processing data other than name, surname, address, telephone number, and email address.[8]

Notice and consent requirements often create the illusion, but not the reality, of meaningful consumer choice.[9] At the stage of assessing the lawfulness of consent, it is crucial that all the above criteria are fully satisfied.

3. Consent in Practice

Cases where consent is considered a lawful basis for data processing are primarily encountered in the private sector. The main reason for this is that in the public sector, it is rarely possible to imagine a specific situation in which consent requested by a public sector would not be perceived by the data subject as having a compulsory nature, taking into account both direct and indirect influence and the anticipated impact of the data controller.

A similar risk may exist regarding the lawfulness of the data subject's consent when the data subject is an employee and the processing is carried out by the employer. In this case, the subordinate position is evident, and accordingly, there is a real risk that the data subject's decision regarding a particular process may be associated with certain pressure and may negatively affect their expressed will and attitude.

However this does not mean that employers can never rely on consent as a lawful basis for processing. There may be situations when it is possible for the employer to demonstrate that consent actually is freely given. Given the imbalance of power between an employer and its staff members, employees can only give free consent in exceptional circumstances, when it will have no adverse consequences at all whether or not they give consent.[10]

When requesting consent, data controllers have considerable leverage, the unlawful formulation and "covert" nature of which, even when brought to the attention of the data subject, may result in the obtained consent lacking legal effect. In such cases, it may be determined that the data controller actually carried out the specific data processing without a lawful basis.

[7] Ibid, Article 6(1)(a).
[8] Ibid, Article 12(2).
[9] *Cate, F. H.* The Failure of Fair Information Practice Principles In *Consumer Protection in the Age of the Information Economy,* 2006, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1156972> [27.11.2025].
[10] *European Data Protection Board (EDPB),* Guidelines on consent under Regulation 2016/679,2018, 7, <https://www.edpb.europa.eu/sites/default/files/files/file1/20180416_article29wpguidelinesonconsent_publish_en.pdf> [27.11.2025].

It is important to emphasize, that: "If a controller seeks to process personal data that are in fact necessary for the performance of a contract, then consent is not the appropriate lawful basis."[11]

Of course, this excludes situations in which the data controller seeks a lawful basis for the processing and considers the data subject's consent in their actions, such as silence, inaction, pre-ticked boxes, or the blanket acceptance of initial settings, rules, and terms and conditions.

It is often argued that treating the data subject's consent as a lawful basis for data processing may pose legal and practical risks. These risks may occur even if the data controller provides full information. In his work "The Practical Failure of Fair Information Principles," American data protection and privacy expert Fred H. Cate identifies one of the main difficulties in implementing information provision in practice: the general public's disregard for provided privacy policies and information. As data protection laws and regulations become more complex, the notices required by those enactments also increase in complexity.[12]

Similar risks are also addressed by the European Data Protection Board (EDPB) in its guidelines on consent, which note the dangers that arise when data subjects frequently provide consent without being adequately informed of the forms used to obtain it. As a result, a real risk is created for them, since consent is often requested for processing activities that would not be lawful without the expression of their explicit will.[13]

These circumstances, in turn, increase the risks associated with the lawfulness of consent.

3.1. Consent of a Child

The importance of lawful processing of a child's data is also evidenced by its regulation under special rules. Under Georgia's national legislation, as well as international standards, particular attention is paid to protecting the rights of a child and implementing effective mechanisms for their realization. This is primarily due to the inherent characteristics of children themselves, including their potentially incomplete understanding of the issue, inability to fully assess their best interests, and inability to fully perceive associated risks, which constitute a non-exhaustive list of circumstances that justify a high standard of protection for their rights.

[11] *"EDPB",* Guidelines 05/2020 on consent under Regulation 2016/679, 10, <https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf> [27.11.2025].

[12] *Cate, F. H.* The Failure of Fair Information Practice Principles In Consumer Protection in the Age of the Information Economy, 2006, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1156972> [27.11.2025].

[13] *EDPB,* Guidelines 05/2020 on consent under Regulation 2016/679, 19, <https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf> [27.11.2025].

The Swedish Authority for Privacy Protection places particular emphasis on the protection of children's rights in the online environment. "Children and young people move quickly and expertly between various platforms, but this does not always mean that they realise the risks or understand the consequences – consequences that may be far away in the future."[14]

When obtaining consent from a child, the data controller must exercise particular care to ensure that the consent request is presented in a simple, comprehensible language suitable for a child, and, if necessary, supplemented with additional visual aids.[15] The Data Protection Commission (DPC) also discusses several examples of such measures: cartoons, videos, pictures, images, and game-related elements—adapted to the age groups of users—and considers them effective means of conveying information to children.[16]

The Law of Georgia on Personal Data Protection also provides for a different regulatory approach when it comes to special category data of a child.[17] In such cases, in addition to the high risk associated with children, the characteristics of the data itself require a high standard of protection. Specifically, processing special category data of a child is permissible under the law only with the written consent of the parent or legal guardian, unless otherwise provided by law.[18]

3.1.1. Consent of a Child – International and National Practice

The European Union's General Data Protection Regulation (GDPR), as well as Georgia's national legislation, provides for special regulation regarding the processing of a child's data. Specifically, in these cases, the relevant threshold age is considered to be 16 years, at which point the data subject is granted the right to manage their personal data and consent to specific processing activities.[19] For a full understanding, it should be noted that there are exceptions to this rule where the law directly specifies a different regulatory approach.[20]

Additionally, Georgia's legislation imposes strict requirements to ensure a high standard of protection when processing children's data, setting the minimum age for

[14] *Swedish Authority for Privacy Protection*, The rights of children and young people on digital platforms, Stakeholder guide, 3, <https://www.imy.se/globalassets/dokument/rapporter/the-rights-of-children-and-young-people-on-digital-platforms_accessible.pdf> [27.11.2025].
[15] *The Autoriteit Persoonsgegevens (AP),* Legal Basis of Consent, <https://www.autoriteitpersoonsgegevens.nl/en/themes/basic-gdpr/gdpr-basics/legal-basis-of-consent> [27.11.2025].
[16] *Data Protection Commission (DPC),* Fundamentals for Child-Oriented Approach to Data Processing, December 2021,29, <https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf> [27.11.2025].
[17] Law of Georgia on Personal Data Protection 14/06/2023, Article 7(3).
[18] Ibid., Article 7(1).
[19] GDPR, Article 8 (1)
[20] Law of Georgia on Personal Data Protection 14/06/2023, Article 7(1).

giving consent to data processing at 16,[21] whereas Article 8 of the EU General Data Protection Regulation (GDPR) allows member states to set the minimum age at no less than 13 years.[22] This difference reflects Georgia's inclination to maintain a stricter standard for the protection of children's data.

In contrast to this approach, the United Kingdom's UK General Data Protection Regulation (UK GDPR) adopts a more flexible regulatory approach, establishing that the minimum age for giving consent to the processing of a child's data is 13 years.[23]

In the guide "The rights of children and young people on digital platforms" Swedish Authority for Privacy Protection notes, when discussing consent given by persons aged 13 to 16, that: "it needs to be assessed in each individual situation if the child in question can be considered able to understand the consequences of consent. Factors influencing this assessment include how sensitive the personal data provided by the child are, how long they will be saved, as well as the age and maturity of the child."[24]

The French data protection authority (CNIL — Commission nationale de l'informatique et des libertés), when addressing the protection of child's personal data, also emphasizes the importance of parental control mechanisms."Children are not necessarily able to fully understand the risks they face online and make informed decisions. Parents need effective tools to support them in their online lives."[25] However, attention is also drawn to the need for caution to ensure that the control mechanism is not excessively intrusive, so that its use does not lead the children to feel under constant supervision.[26]

The French data protection authority's (CNIL) recommendation also defines the need for parental control mechanisms to comply with data protection regulations. "Any proposed parental controls must comply with data protection rules, and in particular with:

- The **principle of proportionality** taking into account the child's interests, age and level of maturity, and avoiding the use of intrusive features such as constant tracking;
- The **principle of transparency** towards the child by clearly explaining which parental controls are being used;

[21] Ibid.
[22] GDPR, Article 8 (1).
[23] UK General Data Protection Regulation (UK GDPR), Article 8 (1).
[24] *Swedish Authority for Privacy Protection*, The rights of children and young people on digital platforms, Stakeholder guide, 20, <https://www.imy.se/globalassets/dokument/rapporter/the-rights-of-children-and-young-people-on-digital-platforms_accessible.pdf> [27.11.2025].
[25] *CNIL (Commission nationale de l'informatique et des libertés), Recommendation 5: Promote parental controls that respect the child's privacy and best interests,* 09 August 2021. <https://www.cnil.fr/en/recommendation-5-promote-parental-controls-respect-childs-privacy-and-best-interests> [27.11.2025].
[26] Ibid.

- The **principle of security** of the child's data, in order to ensure that third parties do not have access to information about the child (e.g. the child's geolocation data). "[27]

When discussing the issue of parental/guardian control over children, the Swedish Authority for Privacy Protection notes that they must not be subjected to unlawful or arbitrary restrictions on their personal and family lives. Those exercising control bear responsibility for the child's upbringing and development, taking into account the child's best interests. In this context, a particularly important task is to balance the existing interests and to be aware of their significance.[28]
"The older the child is, the greater consideration must be given to the child's own will and consent"[29].

3.2. Consent in a Document Regulating Multiple Issues

When selecting the data subject's consent as the legal basis for data processing, the data controller must exercise particular care and attention when consent is included as part of a document that, in addition to the mentioned matter, also regulates other issues.

In this case, it is particularly important that the consent text in the relevant document is formulated clearly, in simple and understandable language, and also separated from other parts of the document.[30]

A similar requirement is provided in the European Union General Data Protection Regulation (GDPR)**,** specifically Article 7(2): "If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language."[31]

This requirement is based on the principle of transparency in data processing. The data subject must clearly understand exactly which processing activities they are consenting to, which data will be processed, for what purpose, and on what legal basis. Any consent form that is not visible, not separated from the full text of the document, and, by reasonable assessment, is not perceived as a choice given by the data subject regarding the management of their personal data, must be excluded**.** Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.

[27] *CNIL (Commission nationale de l'informatique et des libertés), Recommendation 5: Promote parental controls that respect the child's privacy and best interests,* 09 August 2021, <https://www.cnil.fr/en/recommendation-5-promote-parental-controls-respect-childs-privacy-and-best-interests> [27.11.2025].
[28] *Swedish Authority for Privacy Protection*, The rights of children and young people on digital platforms, Stakeholder guide, 40, <https://www.imy.se/globalassets/dokument/rapporter/the-rights-of-children-and-young-people-on-digital-platforms_accessible.pdf> [27.11.2025].
[29] Ibid.
[30] Law of Georgia on Personal Data Protection 14/06/2023, Article 32(1).
[31] GDPR, Article 7 (2).

3.3. Consent in a Contract

The principle of transparency is particularly important when the document through which the data subject's consent is obtained constitutes a contract.

In this context, the voluntariness of consent is especially sensitive. Consent included in a contract must ensure that the data subject can freely exercise their will, make an informed choice, and that their decision does not affect the terms of the contract, including the decision to enter into or refrain from entering into the contract.

When consent is given in the context of a contract or the provision of a service, the assessment of voluntariness must take into account, among other factors, whether consent is a necessary prerequisite for the contract or service, and whether the contract or service can be provided without such consent.[32]

This regulation corresponds to the approach of the European Union General Data Protection Regulation (GDPR), which emphasizes that when giving consent for data processing, the data subject's will must be clearly expressed, and that it must not cover data processing that is not necessary for the performance of the contract.[33]

3.4. Consent in the Online Environment

In parallel with the ongoing digitalization of today's reality and the growing use of online services, the number of risks associated with consent obtained from the data subject for the processing of personal data on online platforms is also increasing. The legality of consent obtained through websites, mobile applications, and online services constitutes one of the most relevant and problematic issues.

The European Data Protection Board (EDPB), in its guidelines on consent, addresses the specificities of the digital environment and the associated risks. In particular, in online contexts, data subjects are routinely confronted with numerous consent requests, often expressed through the ticking of buttons or clicking of links. The frequency of such actions may result in a habituation effect, whereby the data subject's vigilance and attentiveness are reduced due to excessive interaction with consent mechanisms. Consequently, there is a real risk that consent may be provided without full awareness, particularly where it is requested for processing activities that would not otherwise be lawful without the data subject's explicit expression of will.[34]

Despite the fact that even in the online environment it is mandatory to comply with legally established criteria and requirements for consent, in practice, there are frequent cases where the form of requesting consent is purely formal. This harmful

[32] Personal Data Protection Service of Georgia, Guideline Recommendation on "Obtaining Consent from the Data Subject," 21.
[33] GDPR, Article 7 (4).
[34] *EDPB,* Guidelines 05/2020 on consent under Regulation 2016/679, 19, <https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf> [27.11.2025].

practice is especially common regarding the regulation of pre-existing records "cookie files" on websites. Upon visiting a website, joint consent forms for existing cookies are often presented, whereas the data subject has the right to make a choice and consent to the processing of their data only for those cookies they desire, or for cookies that are necessary for the functioning and security of the website, and therefore are essential for its operation.

Furthermore, it is important that consent is obtained upon entry to the website**,** before cookies or other data are placed on the user's device, for example through cookie banners. Consent must be separate for each purpose of data processing (e.g., advertising, analytics, etc.), and the data subject must provide it individually**.**[35]

In addition, the legally defined criteria for consent acquire particular importance in the online environment. In particular, the principles of transparency and informed consent require that the information provided to the data subject be clear, understandable, and specific.

In the context of online consent, an interesting discussion can be found in one of the decisions of the Court of Justice of the European Union (CJEU) in Planet49 GmbH (C-673/17, 1 October 2019)**,** which states that in such cases:" it would appear impossible in practice to ascertain objectively whether a website user had actually given his or her consent to the processing of his or her personal data by not deselecting a pre-ticked checkbox nor, in any event, whether that consent had been informed. It is not inconceivable that a user would not have read the information accompanying the preselected checkbox, or even would not have noticed that checkbox, before continuing with his or her activity on the website visited"[36]

Consent obtained in the online environment must itself be obtained through active action (clicking a button, checking a box, etc.), which excludes the legal validity of consent obtained through pre-checked or automatically selected forms**.**

3.5. Right to Withdraw Consent

One of the guarantees of the voluntary nature of consent is also the possibility to freely withdraw consent and the provision of information to data subjects about this right. Similar to the provision of information on data processing in advance, information regarding the withdrawal of consent must also be provided prior to the data subject giving consent**.**

The regulation of the right to withdraw consent is addressed in several provisions of the Law of Georgia on Personal Data Protection**.**

Direct Marketing – Article 12 of the Law of Georgia on Personal Data Protection[37] establishes the obligation to provide information on the right to withdraw consent and

[35] Personal Data Protection Service of Georgia, "Guide for Individuals Interested in Creating a Website", 27.
[36]European Court of Justice, CJEU, Case C-673/17, Planet49 GmbH [2019], §55, <https://curia.europa.eu/juris/document/document.jsf?text=&docid=218462&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=143828> [27.11.2025].
[37] Law of Georgia on Personal Data Protection 14/06/2023, Article 12(3).

the guarantees for the exercise of this right, specifically in terms of its free of charge and unrestricted use.

Chapter on Data Subject Rights – Article 20 of the Law of Georgia on Personal Data Protection[38] details the necessary preconditions for the exercise of this right:

- **Without temporal limitation, at any time** – this excludes the possibility for the data controller to set any specific time frame for requesting consent, even by specifying and justifying their particular purpose.
- **Without explanation or justification** – to implement effective measures for the realization of the purposes of the law and the fundamental rights of the data subject, it is important to guarantee the possibility to withdraw consent without providing justification or explanation.
- **Using the same means by which consent was given** – the criterion of voluntariness and free exercise of will implies that the data controller must not apply any influence, pressure, or obstacles that would artificially prevent the exercise of this right, and must ensure that consent can be withdrawn in the same manner it was given.

Moreover, when assessing the lawfulness of consent, the burden lies with the data controller to demonstrate that the exercise of this right by the data subjects is not associated with any particular costs and, accordingly, does not entail an obvious risk of negative consequences.[39]

When assessing the ability to exercise the right to withdraw consent freely and at any time, attention must also be given to the specific characteristics of the process. „If you would not be able to fully action a withdrawal of consent – for example because deleting data would undermine the research and full anonymisation is not possible – then you should not use consent as your lawful basis (or condition for processing special category data). Consent is only valid if the individual is able to withdraw it at any time.) “[40].

3.6. Withdrawal of Consent in the Online Environment

In the online environment, in addition to issues related to obtaining consent, it is important that the possibility and the right to withdraw consent are taken into account and effectively implemented in practice.

[38] Ibid., Article 20.
[39] *EDPB,* Guidelines 05/2020 on consent under Regulation 2016/679, 13, <https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf> [27.11.2025].
[40] *Information Commissioner's Office (ICO),* “What is Valid Consent?” <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/consent/what-is-valid-consent/> [27.11.2025].

For the full exercise of this right by the data subject, it is necessary that the digital environment and its specificities in practice comply with the requirements of the law. Establishing complex and multi-step procedures for withdrawing consent on a website directly indicates a lack of good faith on the part of the data controller and inconsistent respect for the rights of the data subject.

Consent should not be limited to a technical form or a mere click of a button — it must represent a genuine expression of will, based on the principles of transparency**,** being informed**,** and freely exercised choice**.**

4. International Practice and Challenges

The issue of considering consent as a legal basis for data processing, as well as its compliance with the law and the effective exercise of related rights, represents one of the current topics in international law. Analysis of practice shows that particular importance is attached to the principles of voluntariness**,** being informed**,** and transparency**.**

Furthermore, analyzing international practice provides an opportunity to assess the compliance of national legislation with international standards, to identify existing challenges, and to evaluate potential risks based on comparative analysis.

4.1. European Union (GDPR)

An important role in establishing international practice is played by Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, the General Data Protection Regulation (GDPR),[41] which defines the principles, rights, and obligations related to data processing, aimed at protecting the personal data of natural persons.

GDPR assigns particular importance to and clearly distinguishes the following mandatory characteristics of consent:

- Clear affirmative action
- Voluntariness
- Specificity
- Being informed
- Clarity[42]

In addition, GDPR provides for the burden of proof on the data controller**,** who must be able to demonstrate that consent was obtained for the data processing operation.[43] Furthermore, the regulation clearly highlights the risks arising when there

[41] 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
[42] Ibid., Recital 32.
[43] GDPR, Article 7(1).

is an apparent imbalance of power between the data controller and the data subject, particularly when the data controller is a public authority.[44]

Analysis of the consent-related provisions under GDPR reveals a clear similarity to the provisions of Georgian legislation and a comparable approach in regulatory practice. Specifically, in the examined cases, a uniform approach to expressing consent in a written document is observed, even when the document also regulates other matters. In discussions of the issue, it is clearly defined, in accordance with both national and international legislation, that the consent text/declaration must be separately distinguished from other matters and presented in a clear and easily understandable language**.**

There is also a direct correspondence between Georgian national legislation and GDPR provisions regarding the requirement to obtain consent. In both cases, the possibility to request consent freely and without limitation is considered a precondition for the correct formulation of consent and its implementation as a legally valid basis.[45]

International practice, particularly the provisions of GDPR, constitutes an important standard on which Georgian legislation and practice rely for guidance. International regulations demonstrate how the text requesting consent should be formulated to ensure the principles of voluntariness**,** being informed**,** and transparency**.**

Accordingly, GDPR serves not only as an educational and guidance instrument in the field of data protection, including in determining the lawfulness of processing operations, but also as a significant standard that supports the refinement of national legislation and the enhancement of current practice and legal awareness within society.

5. Conclusion

When considering the issue of consent as a legal basis for data processing, and evaluating the related statutory requirements and criteria, it becomes clear that what may initially appear as the simplest and most suitable basis for processing is, in fact, sufficiently complex and multifaceted. The associated protective mechanisms fully exclude the possibility of consent existing merely in a formal sense.

For the effective functioning of the consent institution, a combination of several factors is decisive — transparency**,** being informed**,** voluntariness**,** and the good faith of the data controller. When these criteria are collectively ensured, it can be concluded that the data subject's consent genuinely represents a free expression of will, rather than mere formality.

[44] Ibid., Recital 43.
[45] Ibid, Article 7(3).

The Information Commissioner's Office (ICO) establishes a general principle regarding the lawful basis of consent, according to which, whenever meeting the standard for consent is difficult, this is a sign that consent may not be an appropriate basis for data processing.[46]

In the contemporary digital environment, where the volume and frequency of data processing are unprecedented, particular importance is attached to the practical provision for obtaining and withdrawing consent — the user must be able to easily understand what they are consenting to and, if desired, withdraw it.

In the long term, it is essential that the consent institution does not become a formalistic mechanism, but rather serves as a real guarantee of the individual's awareness and freedom of choice. Establishing such an approach ensures the development of a data protection culture, effective application of legislation, and the strengthening of public trust in both the public and private sectors.

[46] *Information Commissioner's Office (ICO),* Guideline on *When is consent appropriate?* https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/consent/when-is-consent-appropriate/

Bibliography:

1. Law of Georgia on Personal Data Protection 14/06/2023.
2. Guideline Recommendation of the Personal Data Protection Service of Georgia on "Obtaining Consent from the Data Subject," 10, 21.
3. Personal Data Protection Service of Georgia, "Guide for Individuals Interested in Creating a Website," 27.
4. EU, 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).
5. UK General Data Protection Regulation (UK GDPR), <https://www.legislation.gov.uk/ukpga/2018/12/contents> [27.11.2025].
6. *The Autoriteit Persoonsgegevens (AP),* Legal Basis of Consent, <https://www.autoriteitpersoonsgegevens.nl/en/themes/basic-gdpr/gdpr-basics/legal-basis-of-consent> [27.11.2025].
7. *Cate, F. H.* The Failure of Fair Information Practice Principles In Consumer Protection in the Age of the Information Economy 2006, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1156972> [27.11.2025].
8. *CNIL (Commission nationale de l'informatique et des libertés),* Recommendation 5: Promote parental controls that respect the child's privacy and best interests, 09 August 2021, <https://www.cnil.fr/en/recommendation-5-promote-parental-controls-respect-childs-privacy-and-best-interests> [27.11.2025].
9. *Data Protection Commission (DPC),* Fundamentals for Child-Oriented Approach to Data Processing, December 2021, 29, <https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf> [27.11.2025].
10. *European Data Protection Board (EDPB),* Guidelines on consent under Regulation 2016/679,2018, 7, <https://www.edpb.europa.eu/sites/default/files/files/file1/20180416_article29wpguidelinesonconsent_publish_en.pdf> [27.11.2025].
11. *EDPB,* Guidelines 05/2020 on consent under Regulation 2016/679, 10, 13, 19, <https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf> [27.11.2025].
12. *Information Commissioner's Office (ICO),* Guideline on What is valid consent? <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/consent/what-is-valid-consent/> [27.11.2025].
13. *Information Commissioner's Office (ICO),* Guideline on When is consent appropriate? <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/consent/when-is-consent-appropriate/> [27.11.2025].

14. *Swedish Authority for Privacy Protection*, The rights of children and young people on digital platforms, Stakeholder guide, 3, 15, 20, 40, <https://www.imy.se/globalassets/dokument/rapporter/the-rights-of-children-and-young-people-on-digital-platforms_accessible.pdf> [27.11.2025].
15. European Court of Justice, CJEU, Case C-673/17, Planet49 GmbH [2019], §55, <https://curia.europa.eu/juris/document/document.jsf?text=&docid=218462&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=143828> [27.11.2025].