Giorgi Khorbaladze[*]

Processing of Personal Data of a Data Subject through Disclosure on Social Networks

The development of information technologies, while offering numerous opportunities, has also introduced significant risks, particularly those affecting the right to privacy. Data processing in the online environment is becoming increasingly widespread. Of particular importance is the processing of personal data through disclosure on various social networks and digital platforms. Such processing is not considered unlawful provided that it complies with the requirements of personal data protection legislation.

The purpose of this paper is to examine, through practical examples, the specific characteristics of data processing by means of disclosure on social networks and to identify the conditions and criteria under which such processing may be deemed lawful.

Keywords: *Data subject, data controller, data processing, social networks.*

1. Introduction

With the rapid development of information technologies, the legality of personal data processing has become an increasingly relevant issue. Despite the inherent challenges, risks, and threats associated with automated data processing, data subjects often publish their personal information online without considering the possibility of unwanted processing by others. When their rights are violated, they may seek remedies through the relevant authorities, authorized persons, or the courts.

The Law of Georgia "On Personal Data Protection" does not provide an exhaustive list of forms of data processing; any action performed on personal data is, in itself, considered processing. This study does not aim to provide a comprehensive review of all forms of data processing on social networks. Rather, it focuses on the most common form: the disclosure, publication, distribution, or otherwise making personal data publicly available online. The scope of this study is further narrowed by focusing on the identification of the data controllers, specifically examining cases

[*] Master of Laws (LL.M.), Ivane Javakhishvili Tbilisi State University; Senior Lawyer of Presidents Office, Personal Data Protection Service of Georgia.

where individuals, rather than public or private institutions, process personal data. This focus is justified by the fact that national data protection legislation allows individuals to process personal data for clearly personal purposes and/or within the context of family activities without being fully bound by the requirements of the Law of Georgia on Personal Data Protection. Consequently, this study highlights cases where the right to privacy and personal data protection takes precedence over other rights and explores how the law applies to specific instances of individual data processing.

The paper analyzes the legal aspects of personal data processing by individuals on social networks through disclosure, drawing on theoretical frameworks, relevant practices of the Personal Data Protection Service, approaches of data protection supervisory authorities, and case law from the European Court of Human Rights. In addition, it examines the legal basis for processing personal data on social networks, instances of data processing within entrepreneurial and economic activities, features of processing during professional activities or official duties, and processing for clearly personal or family-related purposes.

2. Legal Basis for Processing Personal Data through Social Networks

The requirements of the Law of Georgia on Personal Data Protection do not apply to natural persons who process personal data for clearly personal purposes and/or within the context of family activities. Under current legislation, such processing may include a natural person's online activity on social networks. However, in certain cases, a natural person may still be subject to the Law on Personal Data Protection when their actions on social networks fall within entrepreneurial, economic, professional, or official duties. For example, if an individual discloses another person's personal data on a social network while simultaneously acting in a professional or business capacity, the law will apply, and the individual will be considered the data controller or data processor.

If the processing by a natural person does not fall within the statutory exceptions, the data controller is obliged, during an examination by the Personal Data Protection Service, to justify the legal basis for processing in accordance with Articles 5 or 6 (in the case of special categories of data) of the Law on Personal Data Protection.

A universal legal basis for processing personal data is the oral or written (including electronic) consent of the data subject, when the data are obtained directly from them. However, if the consent does not specifically authorize the controller to disclose the data on a social network, the processing will be considered incompatible with the original purpose. In such cases, the controller must rely on another legal basis provided by law. It is difficult to envisage a scenario where the data subject's consent would justify disclosure on a social network if the data subject objects to the processing.

Of particular interest is the case in which the processing of personal data is based on the circumstance that the data subject has previously made their own data public, and in the case of special categories of data, has done so without an explicit prohibition on use. In this regard, one case studied by the Personal Data Protection Service during an unplanned inspection, concerning data processing on the above-mentioned grounds, is particularly relevant. According to the circumstances of the case, the data subject posted a video on the social network TikTok in which they discussed the benefits of a certain product. Part of the distributed video, which contained the applicant's personal data (visual image and voice), was reposted by a natural person who owns accounts on Facebook, Instagram, and TikTok. The applicant explained that the account owner used the video containing their personal data for commercial purposes (product advertising) without permission, posting it on their own TikTok account, which had more than 500,000 followers. According to the controller, they were selling the product advertised by the data subject online and posted the video containing the applicant's personal data on various social media accounts to inform the public about the product's availability in Georgia. As a result of the investigation, the Personal Data Protection Service established that the applicant had activated the sharing, as well as the "Duet" and "Stitch" functionalities on the video they posted, which allowed another account owner to create a new video using the original video clip or its fragment. The Service noted that, when posting the video, the applicant should have been aware of the risk that the video could become publicly available and potentially be further processed. It was determined that the data processing was based on the provision in subparagraph "e" of paragraph 1 of Article 5 of the Law, as the data subject had made their personal data publicly available. Accordingly, no violation of the requirements of the Law "On the Protection of Personal Data" was detected in the processing of the applicant's data by a natural person on various social networks.[1]

The publicity of data may also arise from legislation. For example, according to Article 6, Paragraph 1 of the Law of Georgia "On Public Registry,"[2] data registered in the public registry and documentation maintained by the registering authority are considered public. Similarly, the Law of Georgia "On Entrepreneurs"[3] provides for the publicity of certain data. The requirement to make data public may serve purposes such as ensuring the stability of civil turnover. However, regardless of the legislator's objective, the processing of such data should not come as a surprise to the data subject.

In individual cases, the processing of personal data may serve to protect the legitimate interests of the controller or a third party, except where those interests are overridden by the overriding interest of protecting the rights of the data subject,

[1] Decision of the President of the Personal Data Protection Service, No. G-1/107/2025, 3 April 2025 (obtained from the Service as public information).
[2] Law of Georgia on the Public Registry, 820, 19/12/2008, Article 6, Paragraph 1.
[3] Law of Georgia on Entrepreneurs, 875-Vრს-Xმპ, 02/08/2021, Article 13, Paragraph 1.

including minors.[4] The legitimacy of the controller's purpose and the necessity of data processing must be assessed on a case-by-case basis, balancing the interests of all parties to reach a lawful and fair decision. In this context, the Personal Data Protection Service considered a case concerning the disclosure of a data subject's personal data by a natural person on the social network Facebook. According to the circumstances, the parties had concluded an oral agreement in which the data subject, in the context of his entrepreneurial activity, undertook to send vehicles from the People's Republic of China to Georgia for a certain fee to the data controller. The controller argued that the data subject violated the terms of the agreement, as the vehicles consisted of secondary materials/parts and could not be operated. Communication with the applicant to resolve the issue had been unsuccessful. Within the investigation, it was revealed that the controller published the applicant's personal data in the form of a post and screenshots on his personal Facebook account and in one public group. These screenshots included the applicant's Facebook profile page, displaying their name, surname, two photographs (profile and cover photos), and part of their passport photograph. The controller explained that the purpose of disclosing the data was not to discredit or blackmail the applicant but to protect his own interests. Since the applicant had caused material damage to multiple people, the controller aimed to prevent further harm, thereby asserting a legitimate interest in protecting his own and third parties' material interests and informing the public. Accordingly, the controller considered the information disseminated to be proportionate and minimal. He also cited the exercise of his right to freedom of expression. The Personal Data Protection Service recognized the legitimacy of the controller's interest but found that the processing of the applicant's data did not meet the "necessity" criterion. Although the applicant had made some information publicly available on Facebook, creating a legal basis for processing, the controller could have achieved his purpose by less intrusive means, without publishing a screenshot of the applicant's passport. Therefore, despite the right to freedom of expression, the controller was obliged to pursue the protection of property interests and public information in a manner proportionate to the data subject's right to privacy. Based on this assessment, the Service determined that Article 5 of the Law had been violated and imposed an administrative penalty on the controller under Article 67 of the Law.[5]

The Law of Georgia on Personal Data Protection requires that a controller process personal data based on at least one of the legal grounds, an exhaustive list of which is set out in Articles 5 and 6 of the Law. The burden of proving the legal basis for any data processing operation rests with the controller, and its relevance is assessed by the Personal Data Protection Service during the examination of the lawfulness of the processing.

[4] Law of Georgia on Personal Data Protection, 3144-XIმს-Xმპ, 14/06/2023, Article 5, Paragraph 1, Subparagraph "i".

[5] Decision of the Head of the Personal Data Protection Service, No. G-1/259/2025, 23 July 2025 (obtained from the Service as public information).

3. Data Processing within the Framework of Entrepreneurial and Economic Activities

Entrepreneurial activity is a lawful, non-recurring, independent, and organized activity carried out for the purpose of making a profit. It can be conducted either as an individual entrepreneur or as an entrepreneurial society[6]. Economic activity is defined as any activity undertaken to receive income or compensation, regardless of the outcome. [7] Data processing by a natural person within the framework of these activities is not considered an exception to the scope of the Law "On Personal Data Protection." In such cases, the data processing must fully comply with the legal requirements established by the Law.

The Personal Data Protection Service, acting on a notification from the Public Defender's Office of Georgia, examined a case concerning the processing of minors' data on a Facebook page. In this case, data controller registered in the Register of Entrepreneurs and Non-Entrepreneurial Legal Entities as an individual entrepreneur, managed the Facebook page and posted a call to parents or legal representatives of minors to upload photographs of minors in the comments section in order to participate in a photo contest. According to the controller, the contest winner would be determined by the number of "likes" on each photograph and by a specific electronic program at random. It was established that some of the submitted photographs of minors, including images containing naked children, remained publicly accessible on the page even after the contest ended. The Personal Data Protection Service determined that, since the individual was conducting these activities as an individual entrepreneur, the Law on Personal Data Protection applied to the data processing. Although the photographs were posted by parents or legal representatives, the individual was considered the data controller, as he automatically collected and displayed the participants' photos in the course of his entrepreneurial activity. Despite the parents' consent to post the photographs, the Personal Data Protection Service issued a mandatory instruction to data controller requiring the deletion of the photographs and associated comments from the post, in line with the best interests of the minors. In the event of a similar future competition, the controller is required to perform the same deletion task after achieving the relevant goal.[8]

An interesting case arises when it is not the controller who acts within the scope of professional activity, but the data subject themselves, and the processing of data is related to the performance of their official duties. The European Court of Human Rights considered the case Toth and Crișan v. Romania,[9] in which, on 8 April 2016,

[6] Law of Georgia on Entrepreneurs, 875-Vრს-Xმპ, 02/08/2021, Article 2, Paragraphs 2 and 3.

[7] Law of Georgia on the Tax Code, 3591, 17/19/2010, Article 9, Paragraph 1. Approved by the National Statistics Office of Georgia according to the types of economic activities defined in the National Classifier of Georgia. See: <https://www.geostat.ge/media/70150/NACE-Rev_2_GE_2023.pdf> [30.8.2025].

[8] Decision of the Head of the Personal Data Protection Service, No. G-1/269/2025, 1 August 2025 (obtained from the Service as public information).

[9] Case of Toth and Crișan v. Romania, [2025] ECHR, App. No. 45430/19.

police officers (the applicants) fined S.T. and his mother for violating household waste disposal rules. On the same day, S.T., using his personal Facebook account, published a post in a public group, accompanied by a photograph of the applicants taken at the scene. The post described the incident and alleged that the police officers had physically assaulted the mother and daughter in the presence of the child and verbally abused them. The post was followed by responses from group members. In the comments, Facebook users referred to the complainants with derogatory terms (e.g., "idiots," "crazy," "uneducated"), and some identified the officers, citing similar incidents. In his comments, S.T. revealed the name of one of the complainants and stated that he did not intend to defame them.

The applicants applied to the domestic court seeking compensation for non-pecuniary damage and requiring S.T. to issue an apology to local newspapers and the public group, as he had published the photograph and name of one of the applicants without consent. This had led to offensive comments by others and disciplinary proceedings against the applicants by their employer. The domestic courts dismissed the claims, finding that the post was not defamatory, that it conveyed S.T.'s own perception of the event, and that it constituted an exercise of his right to freedom of expression by publicly sharing his dissatisfaction. The courts further held that S.T. could not be held responsible for comments posted by others, which he could not delete or prevent, and that the photograph and names had been publicly distributed. Moreover, the applicants, as public figures, were not depicted in an indecent manner.

The applicants then brought the case before the European Court of Human Rights, alleging a violation of Article 8 of the European Convention on Human Rights. The Court noted that the publication of a photograph constitutes a more substantial interference with the right to respect for private life than the mere disclosure of a name. However, if the publication does not concern political or public debate and relates solely to private matters intended to satisfy personal curiosity, the right to freedom of expression is interpreted more narrowly. The Court outlined the relevant criteria for balancing the right to privacy and freedom of expression: contribution to matters of public interest; the notoriety of the affected person; the person's previous behavior; and the circumstances of taking the photograph, including the content, form, and consequences of the published information. The Court found the publication of the photograph justified, as it confirmed the information presented in the post. Unlike the national courts, the European Court did not consider the applicants to be public figures in the strict sense, but noted that given their roles and activities, they were subject to broader permissible criticism. Accordingly, the public had the right to receive information about professionals serving the community, and the applicants should have expected that, given their status and conduct, their photographs could be taken and further processed. The Court ultimately found no violation of Article 8 of the European Convention on Human Rights.

4. Data Processing in Social Networks in the Course of Professional and Official Duties

The processing of personal data in the course of a person's professional or official duties falls within the scope of the Law of Georgia on Personal Data Protection.

The Personal Data Protection Service examined a case concerning the publication of a video recording of correspondence between individuals on the social network Facebook. In this case, the data subject had entered into an agreement with a composer, under which the composer was to write a song in exchange for remuneration. Due to a violation of the terms of the agreement, the composer, as the data controller published a video recording of the communication on his personal Facebook page. The controller explained that the purpose of publishing the video was to inform the public about the applicant's alleged fraudulent activities and to recover the royalties owed. The Service determined that the publication was related to the professional activities of the controller. However, it concluded that the action did not meet the "necessity" criterion defined in subparagraph "i" of paragraph 1 of Article 5 of the Law, as the composer could have protected his rights without infringing on the data subject's rights—for example, by pursuing legal action. Furthermore, the legitimate interests of third parties and the prevention of non-fulfillment of contractual obligations could have been safeguarded by including appropriate terms in the contract. Based on Article 67 of the Law, the Service imposed administrative liability on the controller and ordered the removal of the video recording containing the applicant's personal data from Facebook.[10]

In another case, the Service assessed the publication of a client's data by a real estate agent in a closed Facebook group of approximately 128,000 members. The agent, as the data controller explained that he had published information about his business relationship with the applicant—including the applicant's name, surname, telephone number, and photo obtained via WhatsApp—to inform colleagues about an allegedly unscrupulous client. The Service determined that, although the data were obtained within the framework of a professional relationship, they did not constitute a professional secret, as no confidentiality agreement existed between the parties. Moreover, the agent could not substantiate a legal basis for processing the data. As a result, the Service found the agent in violation of Article 5 of the Law.[11]

In a further case, an anonymous post in a closed Facebook group included the name and surname of the applicant. An employee of a company subsequently posted a comment in the same thread, clarifying the facts referenced in the anonymous post and naming the applicant as the main figure in the event. The Service assessed the processing of the applicant's data in the comment independently of the anonymous post. It was established that the employee was the head of the company's security service and that his employment contract included an obligation to maintain

[10] Decision of the Head of the Personal Data Protection Service, No. G-1/183/2025, 3 June 2025 (obtained from the Service as public information).

[11] Decision of the Acting Head / First Deputy Head of the Personal Data Protection Service, No. G-1/374/2024, 19 December 2024 (obtained from the Service as public information).

confidentiality. The company and the controller clarified that the comment was posted independently and was not based on company instructions, and that the disclosed information had not been obtained in the course of official duties. The controller also failed to specify a legal basis for the data processing. Consequently, the Service determined that there was no lawful basis for publicly processing the applicant's data and imposed an administrative penalty on the company employee under Article 67 of the Law.[12]

5. Data Processing for a Clearly Personal Purpose and in the Context of Family Activity

The processing of personal data by a natural person for a clearly personal purpose and/or within the context of family activity, as an exception from the scope of personal data protection legislation, was first introduced by the European Union Directive 95/46/EC of 24 October 1995.[13] Following the repeal of that Directive, the same exception was incorporated into the European Union's General Data Protection Regulation (GDPR).[14] A similar provision is reflected in the Law of Georgia On the Protection of Personal Data, which stipulates that the Law does not apply to data processing carried out by a natural person for a clearly personal purpose and/or within the context of a family activity, provided that such processing is not related to entrepreneurial and/or economic, professional activity, or the performance of official duties. Data processing for a clearly personal or family-related purpose may include, among others, personal correspondence, management of contact information, and internet activity (including on social networks) carried out within the scope of such activity.[15]

"When posting on the Internet, a person must understand that he or she loses control over his or her own photo, notes, and/or other personal data."[16] In today's digital environment, the processing of personal data through social networks has become increasingly widespread alongside the advancement of information technologies. Individuals themselves are often the initiators of various data processing activities. It is therefore impossible to consider every instance of online data publication as an unconditional violation of personal data protection legislation. Where the disclosure of personal data on social networks arises from a person's

[12] Decision of the Head of the Personal Data Protection Service, No. G-1/307/2024, 24 October 2024 (obtained from the Service as public information).

[13] European Union Directive 95/46/EC of 24 October 1995, OJ L 281, 23/11/1995, Article 3. See: <https://eur-lex.europa.eu/eli/dir/1995/46/oj/eng> [18.9.2025].

[14] European Union General Data Protection Regulation (GDPR), OJ L 119, 4/5/2016, Preamble, Paragraph 18. See: <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng> [18.9.2025].

[15] Law of Georgia on Personal Data Protection, 3144-XIმს-Xმპ, 14/06/2023, Article 2, Paragraph 2, Subparagraph "a".

[16] *Macuka Y.*, Director of DVI, interview with "LSM", <https://shorturl.at/pKZlH> [14.9.2025].

entrepreneurial, commercial, professional, or service-related activity, the supervisory authority, in accordance with the Law of Georgia On Personal Data Protection, will assess the lawfulness of such processing. In all other cases, the extent to which the processing is "necessary" for achieving the legitimate purpose of the data controller must be assessed individually, based on a range of relevant criteria.

According to the circumstances of one of the cases reviewed by the Personal Data Protection Service, a patient visited a clinic to receive medical services. Dissatisfied with the services provided, he photographed the medical staff and publicly posted the images on the "Google Reviews" platform along with a negative comment. The Service determined that the individual had disseminated personal data online in order to publicly express his opinion, attitude, and assessment regarding the clinic's services, and that the data had not been processed within the framework of entrepreneurial, economic, or professional/service activities. The Service also explained that the legal norms[17] regulating defamation and the protection of personal dignity could potentially apply to the given case. The Civil Code of Georgia protects personal non-property rights, which also encompass information disseminated through social networks. [18] As noted in the law, "Information disseminated by a person through social networks—expressed opinions or recorded data—may violate the rights of others."[19]

Publicly disclosing another person's personal data on social networks and making it accessible to all users does not constitute data processing for a personal purpose and/or within the framework of family activity. This exception applies, for example, to private correspondence conducted via social networks or the sharing of data with close friends or family members, where the personal data of others does not become available to the general public. For the exception to apply, it is essential to assess the number of data recipients. Accordingly, the public disclosure of personal data by an individual—regardless of whether the person acted within a commercial or professional context—immediately excludes the possibility that the data was processed for personal or family purposes. In such cases, the supervisory authority is entitled to examine the lawfulness of the processing. However, within the limits of its mandate, if it is determined that the natural person data controller was clearly exercising the right to freedom of expression (for instance, by expressing a personal opinion or sharing an experience), the supervisory authority may decline to consider the complaint. In such circumstances, the affected party must apply to the court to seek protection of their rights—such as honor, dignity, privacy, personal inviolability, or business reputation—which will often need to be balanced against the counterparty's right to freedom of speech and expression.

[17] Correspondence of the Official Responsible for Ensuring Public Access to Information of the Personal Data Protection Service, No. PDPS 3 25 00015900, 17 September 2025 (obtained from the Service as public information).

[18] Civil Code of Georgia, 786, 26/06/1997, Article 18.

[19] Commentary on the Civil Code, Book I, General Provisions of the Civil Code, Tbilisi, 2017, 112. See: <https://lawlibrary.info/ge/books/giz2017-ge-civil_code_comm_I_Book.pdf> [20.9.2025].

Assessing whether an individual has exceeded the limits of the right to freedom of expression does not fall within the competence of the supervisory authority. This approach was also reflected in the practice of the Icelandic Data Protection Authority, which declined to examine the lawfulness of publishing photographs of a minor on the social network "Facebook." According to the circumstances of that case, a dispute had arisen between the child's parents concerning custody. One of the parents, together with a third party (another social network user), published photographs of the minor on the same platform accompanied by defamatory comments about the other parent. The supervisory authority found that the child was identifiable in the photographs and that, under the GDPR, the publication of both the image and the accompanying comments constituted data processing. The authority concluded that the case did not fall within the scope of personal or family-related data processing, explaining that this exception applies only to closed social network accounts, where posts are accessible to a limited audience rather than the general public. It was established that the child's data had been made accessible to all Facebook users without any restrictions. Accordingly, the GDPR applied to the case. At the same time, the supervisory authority found that the parent who had published the child's data was exercising the right to freedom of expression—namely, by informing the public about his difficult situation related to the custody dispute. On the grounds that it lacked the competence to rule on the restriction of constitutionally guaranteed freedom of expression, the authority determined that the matter was subject to judicial review. Consequently, it rejected the complaint concerning the processing of the child's data on the social network by the parent and the third party.[20]

The Personal Data Protection Service did not consider the processing of another person's personal data by a natural person, through the publication of a video recording on the social network "Facebook," as data processing for a clearly personal purpose. According to the circumstances of the case, the natural person had used the courier service of a company to order food products. Dissatisfied with the company's service due to the late delivery of the order, the customer refused to accept it and recorded a video clip containing the courier's visual image in order to document the complaint. The data contoller subsequently posted the video on his publicly accessible Facebook page. He explained that the purpose of creating and publishing the video clip in a publicly accessible form was to record a claim against the company, not to directly insult the courier. The Service clarified that an action cannot be regarded as being carried out in the context of a clearly private or family activity when its purpose is to make the collected data accessible to an unlimited number of persons. Furthermore, the exception does not apply in cases where the action or activity is at least partially directed toward the public sphere and extends beyond the personal or family context of the data controller. The decision emphasized that while the use of

[20] Decision of the Icelandic Data Protection Authority, No. 2020010552, 17 November 2021. See: <https://gdprhub.eu/index.php?title=Pers%C3%B3nuvernd_(Iceland)_-_no._2020010552> [30.8.2025].

social networks and online activities may fall within the context of personal or family activities, this is only applicable when data exchange occurs within closed groups, without any connection to professional or economic activities. Exclusively private use of such services falls within the scope of the exception, provided that it does not involve the unrestricted publication of personal data on the Internet. The Service also assessed the existence of an important legitimate interest of the data controller and the necessity of data processing to protect that interest (noting that processing is considered "necessary" only when there is no other, less intrusive means of protecting a legitimate interest). The individual data controller failed to substantiate a legal basis for posting the personal data of the courier in a publicly accessible form on his Facebook page. The Service explained that the person had alternative ways to express dissatisfaction with the company that would have resulted in less interference with the courier's right to personal data protection — for instance, by posting the video in a restricted-access format visible only to a limited circle of people, within a closed group, or by contacting the company directly in written form to submit a complaint. Accordingly, the Service found a violation of Article 5 of the Law ("Legal Basis for Processing").[21]

Based on the above definitions, it is evident that data processing for a clearly personal purpose and/or within the framework of family activities cannot be considered to exist when personal data are made accessible to an indefinite number of persons.[22] For example, the publication of a data subject's health information by a natural person on a social network—regardless of the scope of that person's activities—will fall within the scope of the Law. In such cases, the supervisory authority must assess whether there was a lawful basis for processing the data in this manner. In individual cases, the supervisory authority should also assess whether the matter is wholly or partly related to the exercise of the right to freedom of expression by the data contoller. For instance, factors such as the social nature of the processing, any prior relationship between the parties, and the connection between the act of processing personal data and an existing legal dispute may be relevant to this assessment.

Taking into account the approaches established by the Law on Personal Data Protection, it is therefore possible to identify several criteria to guide supervisory authorities in properly assessing such cases.[23] In particular, supervisory authorities should determine whether data processing by a natural person falls within the scope of personal and/or family activities by applying the following criteria:

[21] Decision of the Head of the Personal Data Protection Service, No. G-1/355/2025, 23 September 2025 (obtained from the Service as public information).

[22] According to EU case law, if the purpose of a natural person is to make collected data available to an unlimited circle of persons, then it is not considered data processing for a clearly personal purpose. See: <https://gdprhub.eu/index.php?title=Article_2_GDPR#(c)_Processing_by_a_natural_person_in_the_course_of_purely_personal_or_household_activity> [19.9.2025].

[23] See:<https://gdprhub.eu/index.php?title=Article_2_GDPR#(c)_Processing_by_a_natural_person_in_the_course_of_purely_personal_or_household_activity> [19.9.2025].

- **Data processing environment** – the dissemination of data to an indefinite number of persons through social networks does not constitute processing for a personal purpose;
- **Social context of processing –** the environment in which the individual processes personal data should be taken into account, including the nature of the data subjects and the group of persons who have access to the disseminated information;
- **Necessity of processing –** the processing must be necessary to achieve a legitimate purpose pursued by the individual, such as the exercise of the right to freedom of expression;
- **Nature of the individual's activity –** the processing of personal data carried out within the framework of economic, entrepreneurial, professional, or service-related activities does not qualify as data processing for personal purposes.

6. Conclusion

The development of information technologies, while offering numerous opportunities, has also introduced risks that may impede the effective exercise of personal autonomy and the right to privacy. Data processing in the online space is becoming increasingly widespread, and social network users often share personal data with a wide audience without fully considering the potential risks of unauthorized processing by others. While sharing personal data on social networks is common and often seen as relevant today, it may, from a future perspective, be regarded as imprudent or inconvenient. As noted, "In the Internet space, it is difficult, painful, and sometimes even impossible to delete one's personal data."[24]

When making personal data public, data subjects must exercise utmost caution, as further unauthorized or unwanted processing may conflict with the Law on the Protection of Personal Data. Data protection legislation grants the controller the right to process personal data, for example, when the data subject has voluntarily made such data publicly available. The rights to privacy, family life, private space, and communication are not absolute and may be limited by law or to protect the rights of others. In a democratic society, the competing nature of human rights necessitates a fair balance between individual rights, and it is unjustifiable to safeguard the interests of one party at the expense of another. The limitation of personal data protection legislation to cases of data processing by a natural person for a clearly personal and/or family purpose reflects this aim of maintaining such a balance. The legislator explicitly excluded data processing for personal purposes and/or within family activities from the scope of entrepreneurial, economic, professional, or official duties.Furthermore,

[24] See: <https://www.facebook.com/photo/?fbid=1094114552832861&set=a.181886710722321> [14.9.2025].

national and international data protection practice confirms that the disclosure of other persons' personal data by a natural person on social networks does not constitute data processing for a clearly personal purpose. Consequently, the lawfulness of such actions must be assessed under personal data protection legislation. Importantly, while processing personal data by a natural person through disclosure on social networks often falls within the scope of the Law on Personal Data Protection, it does not automatically imply illegality. Legal grounds for such processing, as provided under the Law of Georgia on Personal Data Protection, may apply, and each case should be assessed based on its specific circumstances.

Bibliography:

1. Law of Georgia on Personal Data Protection, 3144-XIMS-XMP, 14/06/2023.
2. Civil Code of Georgia, 786, 26/06/1997.
3. Law of Georgia on Entrepreneurs, 875-Vრს-Xმპ, 02/08/2021.
4. Law of Georgia on the Tax Code, 3591, 17/19/2010.
5. Law of Georgia on the Public Registry, 820, 19/12/2008.
6. 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.
7. Commentary on the Civil Code, Book I, General Provisions of the Civil Code, Tbilisi, 2017, 112.
8. Correspondence of the Official Responsible for Ensuring Public Access to Information of the Personal Data Protection Service, No. PDPS 3 25 00015900, 17 September 2025 (obtained from the Service as public information).
9. Decision of the Acting President / First Deputy President of the Personal Data Protection Service, No. G-1/374/2024, 19 December 2024 (obtained from the Service as public information).
10. Decision of the President of the Personal Data Protection Service, No. G-1/355/2025, 23 September 2025 (obtained from the Service as public information).
11. Decision of the President of the Personal Data Protection Service, No. G-1/269/2025, 1 August 2025 (obtained from the Service as public information).
12. Decision of the President of the Personal Data Protection Service, No. G-1/259/2025, 23 July 2025 (obtained from the Service as public information).
13. Decision of the President of the Personal Data Protection Service, No. G-1/183/2025, 3 June 2025 (obtained from the Service as public information).
14. Decision of the President of the Personal Data Protection Service, No. G-1/107/2025, 3 April 2025 (obtained from the Service as public information).
15. Decision of the President of the Personal Data Protection Service, No. G-1/307/2024, 24 October 2024 (obtained from the Service as public information).

16. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23/11/1995.
17. *Case of Toth and Crișan v. Romania*, ECHR, App. No. 45430/19, 2025.
18. Persónuvernd (Iceland) - no. 2020010552 [17.11.2021] (<https://gdprhub.eu/index.php?title=Pers%C3%B3nuvernd_(Iceland)_-_no._2020010552> [30.8.2025]).
19. <https://gdprhub.eu/index.php?title=Article_2_GDPR#(c)_Processing_by_a_natural_person_in_the_course_of_purely_personal_or_household_activity> [19.9.2025].
20. <https://www.facebook.com/photo/?fbid=1094114552832861&set=a.181886710722321> [14.9.2025].
21. <https://shorturl.at/pKZlH> [14.9.2025].