Policy paper on

Personal data protection and transparency of political finances

Tbilisi, 2022

Thea Dzimistarishvili

Council of Europe project: „Supporting Transparency, Inclusiveness and Integrity of Electoral Practice and Process in Georgia“

Contents

Introduction

The present study/policy paper and the analysis of applicable legal framework aim to increase transparency of the State Audit Office (SAO) and in particular, SAO Political Finances Monitoring Department, improve good governance and promote best practices for accessibility of public information.

The correlation between transparency of public institutions and quality of democracy has long been recognized by international standards. Information held in public institutions represents public good, access to which is safeguarded by a number of international documents and national legislations. Freedom of information and the right to privacy are concrete rights. Securing a balancing between the freedom of information and the right to the protection of personal data is also an international standard. Many Council of Europe member States have adopted national legislation that requires balancing of the right to the protection of personal data against accessibility of official documents and the duty of confidentiality of professionals.

The present policy paper aims to facilitate the work of the SAO Political Finances Monitoring Department (hereinafter, the Monitoring Department) with regards to the protection of personal data. The document is primarily meant for the SAO Monitoring Department employees, who, in their official capacity, are engaged in processing of personal data of individuals. First of all, the obligation of the SAO as an administrative body to ensure accessibility of information held in official sources according to the procedure and within the timeframe prescribed by law, is important. High quality of SAO transparency is especially important for overcoming the collision between freedom of information and protection of personal data, for which depersonalization of personal data is essential. It is equally important to determine cases when depersonalization of data is required, since personal data usually represent an integral part of information resources, while depersonalization of personal data ensures accessibility of a significant spectrum of information and confidentiality of personal data.

The study addresses all important and problematic legal issues based on the applicable legislation, which should be considered by the SAO and in particular, by employees of the Monitoring Department, for protecting personal data. It therefore provides an overview of the special national legislation, international (with an emphasis on the Council of Europe *acquis*) standards, as well as practice of national courts and the European Court of Human Rights.

International standards for freedom of information and data protection

The right to access information held in public institutions is one of the fundamental and necessary prerequisites of a democratic state. Its significance is far larger than providing individuals with

access to information of their interest. Adequate protection of this right facilitates improved accountability and increased effectiveness of public institutions.

Freedom of information is recognized as a fundamental human right on all continents of the world.[1] „Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers." [2] „Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice." [3]

In addition to UN documents, freedom of information is also safeguarded by regional conventions. According to the European Convention of Human Rights, article 10, „Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers." While some believe that ECHR Article 10 concerns freedom of receiving information (without interference of public authorities), ECtHR case law has made it abundantly clear that it also entails access to information held in public institutions. [4]

Recommendation R(2002)2 of the Committee of Ministers defines in detail principles of accessing official documents, while adoption of the Convention on Access to Official Documents (CETS No. 205) by the Council of Europe on November 27, 2008, marked an important milestone for provision of international guarantees for freedom of information.[5] Following ratification, the Convention will become **the first binding international document** regulating public access to official documents and establishing international standards for transparency of public institutions. According to its explanatory report[6], the principles established by the Convention apply to all agencies exercising administrative functions. The Convention strictly defines cases when access to information can be limited for various reasons (national security and defence, ensuring public order, conducting disciplinary proceedings, protecting the right to privacy and safeguarding other legitimate interests of individuals, etc.) and this should be directly stipulated by law. Such exceptions are subject to „**public interest test**" and „**harm test**", i.e. access to official

[1] UN General Assembly Resolution 59 (I) of 1946
[2] Universal Human Rights Declaration of 1948, article 19
[3] International Covenant on Civil and Political Rights, Article 19
[4] European Court of Human Rights, **Társaság a Szabadságjogokért v. Hungary (no. 37374/05)**
[5] CoE Convention on Access to Official Documents. Georgia became the party to the Convention in 2009, however the Parliament of Georgia has not yet ratified it. Text of the Convention: https://wcd.coe.int/ViewDoc.jsp?id=1377737
[6] Explanatory report of the Convention: http://conventions.coe.int/Treaty/en/Reports/Html/205.htm

information may be denied if the information may harm any of the legitimate interests, except when public interest in openness of such information is more substantial.

Pursuant to the Council of Europe Convention of June 18, 2009, on Access to Official Documents, article 6.2, if a limitation applies to some of the information in an official document, the public authority should nevertheless grant access to the remainder of the information it contains. Any omissions should be clearly indicated.

According to the CoE Convention on Access to Official Documents, a request for access to official documents may be denied, if: a) despite the assistance from the public authority, the request remains too vague to allow the official documents to be identified; or b) the request is manifestly unreasonable.

The CoE Convention on Access to Official Documents also requires public authorities to proactively public information about their official activities.

As noted earlier, CoE Committee of Ministers has prepared a Recommendation to member states on access to official documents.[7] According to the Recommendation, transparency and access to information is important in a pluralistic, democratic society. Wide access to official documents, on a basis of equality and in accordance with clear rules: 1. allows the public to have an adequate view of, and to form a critical opinion on, the state of the society in which they live and on the authorities that govern them, whilst encouraging informed participation by the public in matters of common interest; 2. fosters the efficiency and effectiveness of administrations and helps maintain their integrity by avoiding the risk of corruption; 3. contributes to affirming the legitimacy of administrations as public services and to strengthening the public's confidence in public authorities. Therefore, the utmost endeavour should be made by member states to ensure availability to the public of information contained in official documents, subject to the protection of other rights and legitimate interests.

In EU law, the right to access public documents is established by the Regulation 1049/2001, which provides for public access to European Parliament, Council and Commission documents.

As to data protection law, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108) and Additional Protocol to the Convention (2001) [8] are the first international legal tools concerning data protection.

[7] CoE Recommendation REC (2002) 2 and its explanatory memorandum.

[8] Convention 108 and its additional protocol of 2001 was ratified by the Parliament of Georgia on 28 October 2005 (#2010-IIsss) and on July 27, 2013, respectively (871-rs)

It should be noted that prior to the adoption of the 1981 Convention, protection of personal data used to be viewed within the context of the right to privacy (art. 12 of the Universal Declaration of Human Rights, art. 17 of the International Covenant for Civil and Political Rights, right to the protection of personal data is part of the rights protected by art. 8 of the ECHR, which guarantees the right to respect for private and family life, home and correspondence, and sets the conditions for placing limitations on these rights. The ECtHR jurisprudence makes it clear that the right to the protection of personal data is part of the right to respect for privacy, family life, home and correspondence).

The 1981 Convention has played a very important role in formation of internationally recognized terminology and definitions, and it also imposes a special obligation on member states to adopt corresponding national legislation. Its members include state parties to the ECtHR as well as international organizations. The Convention applies to processing of all types of data, in public and private sectors.

It protects individuals against violations of rights associated with obtaining and processing of personal data, while regulating international flow of personal data. Principles of the Convention include: obtaining and processing personal data fairly and lawfully; storing personal data for a specified and legitimate purpose and not using it in a way incompatible with these purposes; processing of personal data in a manner adequate, relevant and not excessive in relation to the purposes for which they are stored.

As to EU law, Regulation 2016/679 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, known as the General Data Protection Regulation (enacted on May 25, 2018), repealed Directive 95/46/EC. GDPR is directly applicable in EU member states and it does not require to be transposed in the national legislation.[9] It establishes common binding rules that are applicable throughout the territory of the EU for protection of personal data, which excludes radically different regulation of any particular issue.

Following the adoption of the Charter of Fundamental Rights of the European Union in 2001, protection of personal data became a separate, independent right and it was no longer viewed as part of the right to respect for privacy. In particular, in addition to guaranteeing the right to respect for private life, the Charter stipulates the following: Everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other

[9] Georgian translation of GDPR is available on the Data Protection Inspector's website, under International Acts

legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.[10]

According to EU's personal data working group (so-called Article 29 working party) Opinion #02/2016 on the publication of Personal Data for Transparency purposes in the Public Sector, personal data may be processed if the processing is necessary for compliance with a legal obligation to which the controller is subject (the processing must be determined by law).[11] During collection of personal data, a balance should be struck between the right to respect for private life and freedom of expression; collection of personal data must be necessary and proportionate to the legitimate aims pursued. The state needs to be satisfied that: the processing activity is a task carried out in the public interest or it is conducted in the exercise of public authority; the processing operation is necessary for the performance of this task or for the exercise of this authority.

Proportionality, minimisation and other principles

To implement the principles of data processing, the first order of business is to determine the main purposes of the data processing. For example, transparency initiatives may be intended to promote widespread knowledge about the decisions and actions of the government and its administrative bodies, offering basic insights into their processes, operations and personnel. In turn, this allows the public to hold governments to account about the ways in which they perform tasks and manage public resources, thus promoting efficiency and effectiveness. The measures addressed in this Opinion aim to prevent, detect and sanction conflicts of interest, with a view to avoiding the influence of private interests on the exercise of public duties and to strengthen the integrity, objectivity, impartiality of public sector subjects, as well as build up the confidence of citizens in Government.

The proportionality principle should be respected during each processing activity and **especially at the stage of collection and any subsequent publication**. The European Court of Justice has highlighted the importance of a proportionate approach to processing personal data in several cases: "whether stating the names of the persons concerned in relation to the income received is proportionate to the legitimate aim pursued and whether the reasons relied on before the Court to justify such disclosure appear relevant and sufficient"; competent national courts should, "ascertain whether such publicity is both necessary and proportionate to the aim (...), and in particular to examine whether such an objective could not have been attained equally effectively by transmitting the information as to names to the monitoring bodies alone"

[10] EU Fundamental Rights Charter

[11] Article 29 working party – an advisory body on protection of personal data created under the EU Directive

When determining whose data is going to be processed Member States should draw up relevant objective criteria such as: an individual's public power, ability to spend or allocate public money, salary, term of mandate, received benefits, etc. On-line publication of information that reveals irrelevant aspects of an individual's private life is not justified in light of the principles of fairness and proportionality.

Conflict of interest measures generally cover two main processing activities: the exclusive non-public processing of personal data within the competent institutions and on-line publication of certain data. When deciding whether to make information publicly available on-line, competent institutions should always bear in mind the consequences of doing so. It is also relevant to note that what is of interest to the public is not the same as what is in the public interest.

... **Automatic on-line publication** of all the affairs/transactions of the public sector subjects prior to when they took office, **searchable by name and including all details with no distinction based on the nature, type and extent of such data,** may go beyond what is necessary for achieving the legitimate aims pursued.

When considering publication of personal data on-line it is necessary to consider the **potential risks** of such a disclosure. **Where routine or extensive publication is envisaged a privacy, impact assessment is strongly recommended.**

It is also appropriate to consider whether the nature and extent of the personal data being published **may pose risks other than those related to data protection**. For example, publishing personal data related to a data subject's economic situation may make them vulnerable to criminals. That does not exclude the disclosure of these data to competent institutions in charge of collecting and processing these data.

When evaluating whether the processing should include the public dissemination of personal data through on-line publication, different situations should be handled in different ways. Competent institutions may wish to take into account the extent to which the public sector subject concerned is exposed to the risk of corruption, the scope and nature of their actions or tasks (public interest) and the amount of public funds they manage. Generally speaking, it is appropriate to differentiate between politicians/senior public sector subjects and common public sector subjects.

Analysis of national freedom of information and data protection laws

Georgia is among countries that have solidified freedom of information and the right to respect for private life in their constitutions. However, freedom of information as well as the right to the

protection of personal data are not absolute. The possibility to impose limitations on them is provided in nearly all international universal and regional documents, as well as in the Constitution of Georgia. According to the Constitution of Georgia, everyone has the right to freely receive and impart information. Also according to the Constitution, „Everyone has the right to be familiarised with information about him/her, or other information, or an official document that exists in public institutions in accordance with the procedures established by law, unless this information or document contains commercial or professional secrets, or is classified as a state secret...". [12] The focus of this particular constitutional provision is „a subject interested in receiving information from official sources." The Constitution of Georgia allows any interested individual to access information held in state institutions.

The right safeguarded by the Constitution of Georgia allows every member of the society to be informed about issues that are important for him/her and become actively involved in discussions and implementation of issues of central or local significance. All of this serves a general objective of ensuring public access to information held in public institutions, to allow public scrutiny and citizen involvement in activities of the state. To achieve these goals, individuals are allowed to request and receive information that they are interested in, held in public institutions.

To identify the essence of freedom of information, there are a number of notions and institutions that need to be defined. These definitions are provided in Chapter 3 of the General Administrative Code of Georgia (GAC) and they have a special meaning for the purposes of this particular chapter. Notably, the Parliament of Georgia has not adopted a separate FOI law. Instead, FOI provisions are mostly provided in the GAC Chapter 3. We must first of all take into account that freedom of information means access to public information held in public institutions. It is therefore important to provide definitions of public information and a public institution.

An administrative body is a subject that exercises public administration. FOI requirements apply to administrative bodies.[13] Public institutions are defined broadly, based on the functional understanding of administrative bodies, and they also include persons that are delegated by law with certain functions on behalf of a public institution. According to GAC Chapter 3, public institution is defined as a legal entity under private law, financed from a central or a local budget, within the scope of such financing.

[12] Constitution of Georgia, article 18.2.
[13] General Administrative Code of Georgia, Articles 2 and 27

An official document (including a drawing, model, plan, layout, photograph, electronic information, or video- and audio-recording), i.e. any information stored at a public institution, as well as any information received, processed, created or sent by a public institution or public servant in connection with official activities is public. Usually „information" means records or written documents. According to a common practice, FOI is limited to information that already exists in written form. In many Western European countries, FOI applies only to „official documents", which does not include drafts or internal documents.[14]

As noted earlier, FOI is related to the process of public administration. Openness of information is also relevant when a subject is not exercising any functions in the field of public administration but their activities are financed from the central or a local budget. When a subject is not exercising any functions in the field of public administration, no matter how big the interest is in the information related to their activities, the information may not become accessible to everyone. The interest of public scrutiny towards such subjects is legitimate only within the scope of activities that are financed from the central or a local budget.

According to amendments introduced in the General Administrative Code of Georgia, information proactively published by state institutions also falls under the category of public information.

To have an effective system for recording, registering and managing information held in public institutions, it is equally important to disseminate information about the type of data held in a particular institution. To that end, many national legislations include special provisions on recording, registration, management and classification of information.

GAC establishes an obligation to maintain a register of information held in a public institution. According to the law, an institution must enter the information held by them into the Public Register. References to the public information must be entered into the Public Register within two days after receiving, creating, processing or issuing the information. The references must include the name of public information, dates of its receipt, creation, processing and issuance, as well as the name of the natural or legal person, public servant or public institution from which this information was received and/or to which it was sent. [15]

Amendments introduced in the Administrative Code in 2012 have made it possible for public institutions to use unified automated means for managing information. FOI entails not only an individual's right to apply to a public institution with a request for accessing public information of their interest but also, a positive obligation of public institutions to proactively publish

[14] FOI legislation and practice, comparative analysis of foreign legislations and practices, p.17
[15] GAC Article 35

information held by them. The term used in the Administrative Code, „publication" was defined as „entering public information into the Public Register and ensuring availability of public information to the public in the manner determined by law, as well as proactive publication of information." According to the Code, proactive publication entails placing any public information of public interest on electronic resources by a public institution in the manner determined by a respective subordinate normative act. Public institutions are required to designate a public servant responsible for proactive publication of information, while establishment of the procedure for proactive publication of information falls within the scope of regulation of a subordinate normative act to be issued for this particular purpose.

Publication of information based on a public institution's initiative, irrespective of existence of FOI regulations, serves the following two goals: on the one hand, transparency of a public institution will be increased as public will be better-informed about its activities. On the other hand, proactive publication helps decrease the number of requests submitted by interested individuals for accessing otherwise inaccessible public information. As a result, it saves financial and human resources needed for handling such applications.

At the national level, proactive publication is further regulated by the Resolution N219 of the Government of Georgia, dated 26 August 2013. It lists different categories of information subject to proactive publication, including: information about structure of the public institution, its employees, budget, activities, rules, policy, decisions, delegation of powers. According to the same report, **the procedure for submitting a FOI request to a public institution and other information of public interest is subject to publication** (State Audit Service General Auditor's Order N01463/21, dated 7 February 2018, prescribes the procedure for proactive publication of public information and the standard for requesting public information in an electronic form).

The right to access public information entails the right to have a request for public information handled in a timely manner. Receiving information in a timely manner is very important for those seeking information. Often unreasonable timeframes for providing information violate the right to access data of interest held in a public institution. One of the major challenges in FOI practice is delays in providing access to information. According to GAC, a public institution is required to **immediately** provide public information (including information requested in electronic form). This timeframe **may** be extended up to 10 days, if in order to respond to the request, a public institution should: retrieve information from its structural subdivisions in another locality or from another public institution and process it; retrieve and process individual unrelated documents of a considerable size; consult with its own subdivision in another locality or with another public institution. If a ten-day period is required for providing the requested information, a public institution must notify the applicant in advance. Often technical form in which the information is

provided is especially important for applicants. An applicant may choose between several forms in which information can be provided: electronic – emailing the information; transferring the information to an electronic storage device; paper-based copy – by handing the document directly to the applicant or by mailing the document; reading the information at the administrative body; information should be provided in the form which the applicant has requested it.

An applicant should be immediately notified of a refusal of a public institution to provide public information, while within 3 days s/he should be informed in writing of his/her rights and the rules of appealing, as well as of the structural subdivision or public institution that was consulted with in the decision-making process.

What is the difference between creating and processing public information? Does the former also entails the latter? Answers to these questions are extremely important to any individual seeking public information from a public institution. For example, a public institution requests 10 days for providing public information, stating that the information is not available in a single document and processing is required. As a result of processing, a new document will be created from processed data. This leads to the following question: is a document created as a result of processing public information?

According to GAC, a public institution may request 10 days for providing public information if this is required for obtaining and processing individual unrelated documents.[16] As you can see, the Code distinguishes between obtaining and processing of documents. **Therefore, processing of documents entails not only gathering documents in one place or binding the documents but also, processing the data provided in these documents,** i.e., a public institution that receives a FOI request has a very important legal obligation to create a new document. Otherwise, FOI chapter of the GAC will be pointless and an obligation of a public institution will be limited to making mechanical Xerox copies.

Georgian legislation provides a list of different categories of information that are public in any case and may not be classified, including: environmental information, information about risks to their life or health; basic principles and areas of work of a public institution; description of the structure of a public institution, the procedure for determining and distributing employee functions, as well as decision-making procedure, all information related to electing candidates for an elected position; audit reports and auditing results about activities of a public institution,

[16] GAC Article 40.1, subparagraph „b“

as well as court materials for a case where a public institution is a party; aims, scope of use and legal basis for collecting, processing, storing and disseminating data by a public institution, etc.[17]

GAC determines the following categories of secret (classified) information (public information is open, except for cases provided for by law and information categorised as **state, commercial or professional secret or as personal data**). Such information includes information received, processed, created or sent by a public institution or official about official activities, containing personal data, state, commercial or professional secret. Among them, issues related to personal rights fall within the scope of the personal data protection law.

Commercial secret is defined as information on a plan, formula, process or means of a commercial value, or any other information used for manufacturing, preparing, processing of goods or rendering services, and/or is a novelty or a significant result of technical activity, as well as other information that may prejudice the competitiveness of a person, if disclosed. However, there is no automatic classification of information as a commercial secret but instead, a legal procedure must be followed. A company should apply to a public institution and request that information submitted by the company be recognized as a commercial secret. The public institution makes a corresponding decision within the prescribed timeframe. In case of a state secret, classification of information is initiated by the state. The purpose of classifying information as a state secret is to protect vital interests of the state, in strategic areas such as defence, security, foreign intelligence, law and order, economy, etc.

It is very important to highlight the fact that amendments introduced in the GAC on 29 June 2018, **clearly define authority of public institutions to strike a balance between accessibility of public information and the right to the protection of personal data, when there is a prevailing interest to protect rights of others.[18]**

NGOs often criticize the fact that public institutions **tend not to use the balancing test** and when requests concern access to public information that contains personal data, administrative agencies provide such information in a redacted form. In practice, administrative bodies are acting based on the identification criteria prescribed by the Law of Georgia on Personal Data Protection and despite the regulations contained in the GAC, as well as the requirement of art. 5, par. "e" of the Law of Georgia on Personal Data Protection (processing of data is allowed if it is necessary to protect lawful interests of the data controller or a third person, except when there is a prevailing interest of protecting rights and freedoms of the data subject), they automatically classify personal data, without applying „**public interest test**" and „**harm test**" in individual cases.

[17] GAC Article 42.
[18] GAC Article 44.

Therefore, we share criticism of NGOs in that despite applicable legal provisions, the practice of using the balancing test in relation to FOI requests is lacking. As the matter involves conflicting legal values, it is important to consider Supreme Court judgments.[19]

Notably, FOI legislation and practice at the national level is in line with applicable international standards: it is not allowed to charge any fees for accessing public information. It is only possible to charge fees for copies of public record but the fees may not exceed the actual cost of providing that record. Further, fee amount is prescribed by law. Decisions about accessibility of public information can be appealed by anyone and the right to apply to court is guaranteed.

GAC Chapter 3 (freedom of information) prescribes an obligation of public institutions to prepare annual reports about fulfilment of the requirements of the FOI Chapter. The law provides a list of different categories of data that should be included in the report.

As to public information officers, their responsibilities should be determined more clearly (EU law also envisages designating data protection officers in public institutions; [20] in the future, it is possible to have both of these positions combined into one), as it is extremely important for a public information officer to have the authority to make independent decisions. **In practice, a public information officers, who is an employee of the office of correspondence, is only responsible for reviewing an application.**

As noted earlier, issues of accessing public information held in public institutions is regulated by the General Administrative Code and the Law of Georgia on Personal Data Protection. Information held in public institutions is accessible if the law does not impose any limitations on making such information public (the requirement contained by GAC Article 28.1 on limiting access to information that contains personal data), while the Law of Georgia on Personal Data Protection allows access to personal data, if it is provided for by law and is necessary to protect legitimate interests of a controller or a third person (Personal Data Protection Law, subparagraphs „b“ and „e“ of art. 5).

In the field of personal data protection, national legislation is composed of the general law on Personal Data Protection and sectoral laws that ensure protection of data in individual sectors. Compared to the general data **protection** law, special/sectoral data **protection** norms take precedence. The general **data** protection law becomes the main law in absence of special **data** protection regulations.[21]

[19] Supreme Court practice, #as-378-359-2013,2-02.2012. #as-1278-1298-2011
[20] See GDPR Articles 37- 39
[21] Decision of the Supreme Court of Georgia, dated 30 May 2013, case bs-527-518 (k-12)

The Law of Georgia on Personal Data Protection is fully compliant with international data protection standards. It is however desirable to amend the law in view of legislation adopted in the EU recently (concerning the enactment of the General Data Protection Regulation since May 1, 2016).

According to international and national laws, „personal data" means any information relating to an identified or identifiable natural person, i.e. information about a person whose identity is known or can be established after obtaining additional information.[22]

The data protection law defines legal basis and principles for data processing. The purpose of the law is to ensure during processing protection of human rights and freedoms, including the right to respect for private life.

Data processing means any operation performed on personal data whether or not by automated means, such as collection, recording, photographic, audio recording, video recording, organisation, storage, alteration, restoration, retrieval, use or disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.[23]

Inadequacy of legal regulation is clearly illustrated in the afore-mentioned term 'data processing', which entails not only collection, recording, organisation, storage, alteration, restoration, retrieval, use, grouping, combination, blocking, removal and destruction of data but also, their transmission and dissemination.[24] Clearly, an individual's consent to processing of his/her information should not entail transmission and especially dissemination of the processed data, because these actions due to their nature go far beyond the scope of types of processing and represent the kind of actions that should be subject to a stronger protection regime.

It is crucial to observe the following data processing **principles** during processing: **data should be processed fairly and lawfully, without violating dignity of the data subject;** data can be processed only **for specified, explicit and legitimate purposes** and not further processed in a manner that is incompatible with those purposes; data may be processed to the extent of what is necessary in relation to the purposes for which they are processed; data should be adequate and proportionate in relation to the purposes for which they are processed; data should be truthful and accurate and should be kept up to date, where necessary. Data collected and processed without legitimate grounds and in a manner that is incompatible with the purpose of processing should be blocked, deleted or destroyed; data may be stored for no longer than is

[22] European data protection law, a manual by G.Koshadze
[23] Law of Georgia on Personal Data Protection, Article 2
[24] Nugzar Skhirtladze, Legal aspects of personal data protection, p.25

necessary for the purposes for which the data are processed. After the purpose for which the personal data are processed is achieved, the data should be blocked, deleted or destroyed or stored in a manner that excludes identification of a person, unless otherwise prescribed by law.

Notably, failure to observe the principles of data processing as well as processing of data without legitimate grounds leads to an administrative responsibility and relevant sanctions will be applied.[25]

As noted earlier, the law allows processing of personal data if the following circumstances exist: the data subject has provided his/her consent; data processing is provided for by law; processing is necessary for a data controller to perform their statutory duties; processing is necessary to protect vital interests of the data subject; processing is necessary to protect legitimate interests of the data controller or a third person ,except when there is a prevailing interest to protect the rights and freedoms of the data subject; the data are publicly available according to the law or the data subject has made them publicly available; data processing is necessary to protect a significant public interest under the law; data processing is necessary to handle an application of the data subject (provide services to him/her).[26]

Here we should also underline that each form of data processing requires clearly defined purpose. Further processing of data for another purpose that is incompatible with the initial purpose is not allowed. Therefore, when the data subject has given his/her consent, if such data are disclosed/made public, the legislator requires that a separate grounds for processing (one of the grounds listed in art. 5 of the law) should exist.

The first report of the Personal Data Protection Inspector outlines **lack of legal basis** for exchanging data among public agencies and/or providing access to data as a major problem. Clearly, the power to obtain and store data does not automatically entail the right to transfer the data to other agencies.[27]

The problem of accessibility of personal data, protection of their confidentiality is closely tied to an issue of the so-called secondary (routine) use of personal data, which is an exception to the general personal data confidentiality regime and creates a condition for the exchange of personal data between public agencies, if the data is used for the purpose compatible with the purpose of data collection.[28] This exception is provided in the personal data protection law. However, the law

[25] Law of Georgia on Personal Data Protection, articles 43-54
[26] Article 5 of the same law
[27] 2014 report of Personal Data Protection Inspector
[28] Nugzar Skhirtladze, Legal aspects of personal data protection, p.100

does not provide the criteria for compatibility of the purpose and the basis for secondary use of personal data. The issue of compatibility should be decided on a case-by-case basis.

Interestingly, some think that this issue needs to be regulated by law. If necessary, the notion of joint controllers should be introduced (allowing two or more controllers to process data jointly to achieve a common goal). This will certainly promote comprehensive use of data. [29]

Data subject's right to access personal data stored in a public institution about him/her is crucial, **so is the data subject's right to have such data rectified or deleted (the right to be forgotten)**, which are guaranteed by the Law of Georgia on Personal Data Protection.

Practice of international and national courts

In recent years, important interpretations have been made in Georgia's legal doctrine and court practice about the notion of freedom of information. More specifically, freedom of information has been recognized as a fundamental human right in theory and practice and, **although it is closely linked to freedom of opinion and expression, it is now viewed as an independent right.** Court practice clearly shows that the right to access public documents may be confronted with the right to the protection of data, if access to documents in question results in disclosure of personal data of other individuals. Access to information held in a public agency may require striking a balance with the data subject's right to the protection of the data. Interference with the right to the protection of personal data by providing access to official documents requires specific and legitimate grounds and **the right to access official documents will not automatically outweigh the right to the protection of personal data.**

The European Convention of Human Rights (ECHR) has a unique mechanism of control – the European Court of Human Rights, which has been created by the CoE member states to ensure fulfilment of the obligations provided in the European Convention. The Court is authorised to accept and review individual complaints and deliver judgments and decisions that are binding for the parties to the Convention, including for Georgia.

In the case of Társaság a Szabadságjogokért v. Hungary (no. 37374/05), the European Court addressed the issue of striking a balance. The plaintiff was denied access to a complaint pending before court, on the basis that the complaint could not be accessed without its author's approval. National courts ruled that the document contained personal data and protection of personal data could not be overridden by other lawful interests, including the accessibility of public information.

[29] Ibid, p.101

The European Court found a violation of article 10, para.1 of the Convention in this case. It stated that public had the right to receive information of general interest. Given the plaintiff's activities in the field of protection of freedom of information, which included, inter alia, human rights litigation, **the European Court referred to the NGO as a public watchdog and stated that activities of NGOs warrant similar Convention protection to that afforded to the press.** The Court also noted that the submission of an application for review of constitutionality of criminal legislation, especially by a Member of Parliament, undoubtedly constituted a matter of public interest. Consequently, the Court found that the applicant was involved in the legitimate gathering of information on a matter of public importance, and observed that the authorities interfered in the process by creating an unfounded obstacle.

2. L.B. v. Hungary (no. 36345/16) - ECtHR

This case concerned a tax authority publishing personal data of applicants with tax arrears. **The applicant claimed that publication of his personal data did not constitute a necessary measure in a democratic society, it did not serve any legitimate purpose and it was not proportionate to the stated objectives. It therefore infringed his right to private life. The ECtHR did not find a violation in the case.** The Court explained that publication of personal details of major tax defaulters whose tax debts exceeded HUF 10 million was provided for by law, which meant that there was a legal basis for interference with the right to respect for private life. Further, in the Court's view **publication of personal details such as the applicant's name, home address, tax identification number and the amount of unpaid tax did not reach the threshold to have been considered as a violation of the right.**

The chamber judgment was appealed in the Grand Chamber, which is yet to rule on the appeal.

2. Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland (no. 931/13) – ECtHR Grand Chamber

The applicant – an editorial office published newspaper that contained taxpayers' information about their earned and unearned income and assets. Data Protection Ombudsman asked the Data Protection Board to prohibit such publishing of personal data in the newspaper.

The European Court handled the case in light of Article 10 of the Convention and assessed the circumstances against the following criteria: 1. Whether taxpayers had the right to respect for a private life. The Court stated that information collected, processed and published in the newspaper by applicant companies included data about earned and unearned income and assets of taxpayers and therefore, it **clearly concerned personal life of individuals, even though according to the Finnish law, the data was publicly accessible;** 2. Whether the interference had a legitimate goal. In the Court's opinion, the applicants as media professionals/media

representatives should have known that mass collection of data and their dissemination in full may not be considered as processing „solely“ for journalistic purposes. Therefore, the Court found that while prohibition on collection and dissemination of such data amounted to interference of the right guaranteed for journalists by article 10, **it served a legitimate purpose of protecting rights and reputation of others.**

3. Whether the interference was a necessary measure in a democratic society (the Court evaluated the interference against several sub-criteria): **the contribution to a debate of public interest**. The Court noted that although public access to taxpayers' information was subject to clear rules and procedures and to general transparency of the Finnish tax system, it did not mean that publication of the personal data **would contribute to a debate of public interest. When assessing the published information as a whole, similar to the Supreme Administrative Court, the European Court was not satisfied that publication of the taxpayer data in this manner and extent (unprocessed data were published in separate catalogues) ensured such debate or it genuinely served the purpose of contributing to such debate.**

Then the Court assessed **the persons affected**.

It had been established that personal data of around 1 200 000 natural persons had been disseminated, all of whom were taxpayers but only a few of them (public figures or well-known personalities, within the meaning of the ECtHR case law) had high net income. Most data subjects belonged to a low-income group.

The manner of obtaining information and its veracity

In the Court's view, accuracy of the published information had never been disputed between the parties and it had not been established that the personal data had been obtained illegally. The Court however noted that circumstances of the case suggested that the applicants were aiming to circumvent the limitations imposed by law, making the method of obtaining the information questionable.

The content, form and consequences of the publication

It is undisputed that personal information obtained by applicant companies was not publicly available but instead could only be obtained at local tax offices. The journalists could have received tax information in electronic format; however, they could only request a certain amount of data. Journalists should have specified that **the information was requested for journalistic purposes and that it would not be published in the form of a list**. Therefore, in the Court's view, although information about personal data was not secret and could have been requested in the

form of public information, there were specific rules and guarantees that should have been followed.

To the Court, the fact that the disputed data were publicly available according to national laws did not necessarily mean that it could have been published to an unlimited extent. Publication of the data in a newspaper and its further dissemination using a text-messaging service ensured their access in a manner and to the extent not foreseen by the legislator. Guarantees provided in the national law were clearly defined, in view of public accessibility of personal taxation data, the substance and the goal of the data protection law and the nature and the scope of the journalistic derogation.

Sanction

Lastly, the European Court verified the sanction imposed on the applicants to determine if it was excessive and violated their rights.

Violation of Article 10 was not found in this case.

3. **Volker und Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v Land Hessen – Court of Justice of the European Union**

The case concerned publication of information containing personal information of beneficiaries of an agricultural loan provided by the state to farmers.

According to the Court, the right to respect for a private life entails limitations on dissemination of the kind of information that allows identification of a person. The Court of Justice explained that both natural and legal persons had the right to the protection of public data, but with certain differences.

The Court was to assess the issue of striking a balance between the two rights and determine which of the two prevailed: the state's interest to ensure transparency of grants provided or the right of the beneficiaries to the respect for their private life.

The Court noted that protecting transparency is an important goal, however the case file did not include anything to indicate that achieving this goal was possible only by making personal information of the beneficiaries public (in case of natural persons).

However, the Court did not extend the same standard to legal persons and noted that dissemination of their personal data did not violate the proportionality principle. The Court considered that dissemination of personal data harms legal persons and natural persons in different ways. Therefore, the Court did not find publication of information about legal persons to be a disproportionate measure.

Practice of national courts

In the context of the topic of discussion, it is important to refer to practice of the Constitutional Court of Georgia, which has changed recently. More specifically, the Constitutional Court used to exclude from the area safeguarded by the constitutional provision on freedom of information accessibility to any information held in public agencies in relation to private matters of an individual. However, in its judgment №3/1/752 of 14 December 2018, the Constitutional Court found that the provision in the Constitution of Georgia that establishes the right preventing access of third persons to information about private matters of an individual, „does not require that information contained by official records, which are related to an individual's health, finances or other private mattes, be completely closed. To the contrary, the same constitutional provision provides a possibility to limit this right – in cases prescribed by law, when this is necessary „to protect national security or public safety, health, rights and freedoms of others". Therefore, this right may be limited to protect rights and freedoms of others" (Judgment №3/1/752 of the Constitutional Court of Georgia, dated 14 December 2018, in the case of „Non-commercial legal entity Green Alternative v the Parliament of Georgia". Accordingly, pursuant to the Constitutional Court's practice, Artical 18, par. 2 of the Constitution of Georgia protects the right to receive information contained by official documents, including information related to another person's health, finances or other private matters.

According to the Constitutional Court of Georgia, „access to information held in state institutions is an important prerequisite for informational self-determination and the right to free development of a person" (Judgment №2/3/364 of the Constitutional Court of Georgia, dated 14 July 2006, in the case of „Georgian Young Lawyers' Association and a citizen, Rusudan Tabatadze v. the Parliament of Georgia").

Further, interpretations of the Constitutional Court about significance of accessibility of public information and its purpose are worthy of a special note. In particular, „The right to access official documents of the state is directly related to the implementation of open governance in the state and is therefore important for having and maintaining a democratic and pluralistic society. This right entails the state's obligation to create adequate guarantees to make it possible to inform citizens on public issues. Access to official state documents allows interested persons to analyse issues of public importance that they are interested in, ask questions, discuss whether public functions are adequately implemented and become an active participant of the process of making and implementing decisions of public importance. Openness of information promotes accountability of public institutions and increases effectiveness of their work. In an open governance, public agencies/officials expect that their work may be verified by any interested individual and if any irregularities are found, they may be held responsible from legal or political

perspective. Therefore, openness of public information held in public institutions represents an important prerequisite of effective public scrutiny over activities of state agencies. Open governance is essential in a democratic state, to strengthen trust between public institutions and citizens, to prevent and identify in a timely manner violations of law (e.g., corruption, nepotism, misuse of public funds) (Judgment №1/4/757 of the Constitution of Georgia, dated 27 March 2017, in the case of *Giorgi Kraveishvili, a citizen of Georgia v. the Government of Georgia*).

A number of important interpretations were delivered by the Supreme Court of Georgia in disputes over accessibility of public information. In a dispute against Rustavi City Assembly, where the appellant demanded access to information about bonuses received by Assembly officials (individually). The Court pointed that information about bonuses is a private matter of an individual, stating that: „[...] **the requested information allows identification of a person, i.e., it involves personal data. Public information that allows identification of a person constitutes personal data of that person. Therefore, protection of personal data also extends to such information.“** In its judgment, the Court of Cassation noted that **personal data of officials (including candidates for a particular office) and other civil servants are subject to a different standards of protection. „Accessibility of information about officials containing a personal secret serves a legitimate goal – ensuring transparency of information about officials. [...] Therefore, considering the high public interest, data about public officials [...] is open.“** As to bonuses of other public servants, the court established a different standard and noted that because they are not public officials, information about their bonuses constitutes personal data and may not be accessed without consent of the individuals concerned.

In its judgment of 14 September 2017 (case Nbs286-284(k-17), the Supreme Court of Georgia explained: messages sent via work email certainly constitutes public information that exists in **electronic** form and it fulfils the requirements provided by the law for public information. The Court therefore found that the requested information is an „official document“, which does not contain a state, professional and commercial secret.

In its judgment of 23 June 2016, (case Nbs-49-48(k-16), the Cassation Court noted: **accessibility of information is related to the process of implementation of public administration. In order for the process of exercising public authority be transparent, information received, processed, created or sent in relation to official activities should be accessible to everyone. The requirement of openness still applies when the subject does not exercise any public authority but their activities are financed by the central or a local budget.**

The Cassation Court found that information about a **service weapon** of a former Ministry of Internal Affairs employee, model and colour of the weapon and when the weapon was issued to him, **did not constitute personal information. The Court underlined the fact that the person**

concerned used to be an employee of the Interior Ministry and information related to his work may not be considered as personal information subject to protection.

In its judgment of 7 April 2016 (case Nbs-425-418(k-15), the Chamber of Administrative Cases of the Supreme Court of Georgia explained that **work-related information about a civil servant may not be viewed as private information.** In the case in question, the person is already identified. Therefore, information about his work in a public agency may not be considered as identifying information. In order for information to be considered private, the subject should have a reasonable expectation of protection. Working in public service may not be considered as information that falls within the category of private information, which the person concerned may expect to be classified.

In its judgment of 16 January 2020 (case Nbs-s848(k-18), the Supreme Court explained that the legal regime of protection of data of public persons is different from the regime of protection that applies to other individuals. Protection of freedom of information is prioritized over protection of private information concerning **public persons**, as a person who wants to be a public person also declares readiness for possible interferences in his/her private life. An official claiming that **information** in question concerns his/her private life is not proof that the **information** may not be accessed without his/her consent. A person who actively participates in public life should accept that details of his/her private life may become a subject of public or media attention. The cassation chamber highlighted the fact that the requested **information concerned high-level officials, such as the Prime Minister of Georgia, the President, etc**. Opinion of lower instance courts that public has a legitimate interest in having **information** on whether or not high-level state officials have perpetrated violence against their family members and have committed an administrative offence in that regard. It is important that the plaintiff is not requesting access to **information** about the victim of violence, specific circumstances of the incident, or **information** about ongoing proceedings. But rather, the plaintiff's request concerns **information** about the fact of violence by incumbent officials confirmed by relevant authorities.

Georgian Young Lawyers' Association v the Ministry of Defence of Georgia.[30] GYLA was requesting copies of public procurement contracts. The Ministry of Défense of Georgia provided the information in a redacted form. The following was redacted: supplier information (organization, name of the director); cost of services provided; the director's home address and phone number; bank details. GYLA challenged in court provision of information in a redacted from. The court considered legal basis for redacting each data and explained in each case whether the data constituted public information or private information. In its decision, for the

[30] City Court decision of 17 December 2012, #3/3856-12, in which the court did not uphold provision of information in a redacted form.

purposes of freedom of information, the court extended the legal regime to private legal entities, within budgetary financing, noting that: „accessibility of public information is a specific manifestation of effective functioning of a democratic system, ensuring that public has access to information held in public institutions. Public lacks possibility to otherwise receive information about an organization financed by an administrative agency. Therefore, the Ministry of Defence shall, within freedom of information, provide an interested individual with information that falls within the scope of such regulation.“ **Therefore, any legal entity of private law financed from the state budget represents a public institution within the scope of this financing, and their company name should be accessible to everyone.** According to the court, the goal of accessibility of public information would become meaningless and it would have been impossible to actually realize the right to access information. The court also found that name of the organization director was public information, „[...] because both company name and identity (name, last name) of the director (authorised representative) are public. These data are included in the Register of commercial and non-commercial legal entities, which is accessible for all interested individuals.“ An important interpretation was made about value of services concerned: „Accessibility of information on spending of public funds by an administrative agency serves the legal purpose of protecting rights of others. [...] It is the will of the legislator to protect the right of the society and give a private person different functions, meant for public institutions, with regards to finances received and to extend the scope of GAC to it, in order for an outside person, by receiving the requested information, be able to analyse spending of funds allocated from the state budget. Accessibility of the said information serves the purpose of keeping the public informed, to allow it to scrutinize adequacy of spending of the government funds.“ As to the company director's address and phone number, the court explained that this information is private information and even though it was included in the contract, the court did not automatically consider it to be public information because its disclosure would have violated the reasonable expectation of privacy. Therefore, the court rejected the plaintiff's request and it also found that a private person's bank accounts are classified, noting that: „[...] A private person's bank account is information related to financial relationships, and it is meant not for any specific relationship but for pursuing business relationships in general. This kind of information reflects a person's private sphere and concerns financial aspects of his/her work. Therefore, the information falls under the category of financial information of a person, and any private person has constitutional interests of protecting this information, which should be respected.“ This particular decision clearly shows a conflict between the freedom of expression and the right to privacy. On the one hand, the court determined a legal regime for a legal entity under a private law and on the other hand, it prioritized protection of „rights and freedoms of others“ over the right to privacy, in which it considered freedom of information in conjunction with other rights and in particular, transparency of public finances.

Legislation about the State Audit Office, existing practice and recommendations

The State Audit Office (SAO) is a supreme auditing authority. Its powers, rules of operation and organization are determined by the Law of Georgia on the State Audit Office.

According to the Law of Georgia on State Audit Office, SAO main objectives include: **promote legal, efficient and effective spending of public funds and other assets of material value, as well as to contribute to the protection of the national wealth and the property of the autonomous republics and local self-governing units, and to the improvement of the management of public funds.**[31]

SAO (an in particular, the Political Finances Monitoring Department) monitors financial activities of political associations of citizens, within the scope of competencies provided for by the following organic laws of Georgia: The Election Code of Georgia and the Law of Georgia on Political Associations of Citizens. It has the authority to sequester property of natural and legal persons and political associations of citizens (including their bank accounts) and draw up reports on violations of the law and adopt relevant resolutions.

Activities of the State Audit Office are subject to a high standard of transparency, as clearly suggested not only by the regulatory framework, but also by GAC art. 42, par. "g", stipulating that everyone has the right to know about findings of audit reports and revisions about activities of public institutions.

Materials of audit conducted in frames of the SAO competencies, concerning lawfulness of **spending and use of budgetary funds, other State assets of material value,** are publicly available and represent open information.

As noted earlier, the SAO monitors financial activities of political parties. Any party submits to SAO no later than February 1 of every year, the previous year's financial declaration alongside an auditor's (auditing firm's) findings; **the SAO is required to provide to any interested individual with access to information about a party's annual financial declaration and campaign fund account, and to publish it on a corresponding website within 5 working days after it was received.** Notably, SAO develops annual financial declaration form for parties and auditing standards for party financing.

SAO determines the rules related to financial transparency of parties and making of donations (art. 32^2 of the organic law). It also monitors legitimacy and transparency of party financing

[31] Organic law of Georgia on the State Audit

activities. Within the scope of such monitoring, SAO may obtain information about finances of natural or legal persons that have donated to a party, based on a court decision, as appropriate.

Rules regulating transparency of political finances are approved under the order of the SAO General Auditor, establishing reporting rules for monitoring legitimacy and transparency of financial activities of political parties, persons with declared electoral goals, electoral subject candidates, electoral subjects, which is open information.[32]

Here we would like to also note that according to the Procedure for proactive publication of public information and the standard for requesting public information in electronic form, approved by the Order of the SAO General Auditor, proactively published public information is open and equally accessible to anyone.[33] It is not allowed to charge any fees for receiving proactively published information, except for cases prescribed by law; SAO may, within the scope of its competencies and activities, proactively publish other additional public information of public interest.

The Procedure for proactive publication of public information and the standard for requesting public information in electronic form establishes a list of categories of information that should be published proactively: information about donations (in case of a natural person: name, last name, personal number, place of registration); in case of a legal person: name of the organization, identification number, legal address, annual financial declarations, campaign financing reports; statistics of violations and sanctions imposed; interim and final reports of election campaign financing monitoring; normative acts regulating political financing and its monitoring; methodology of monitoring political financing. [34]

Recommendation: It is recommended to implement the following practice at the SAO: analysing statistics about applications submitted to public institutions requesting access to different categories of information, as a credible indicator of what type of additional information represents the subject of public interest and therefore, what type of information of high public interest should be published proactively (in the context of political finances).

In frames of SAO activities, in the process of monitoring financial activities of political associations of citizens, processing/accessibility of data of natural persons (donors) is an important issue.

According to the organic law of Georgia on Political Associations of Citizens, a person making a donation should provide his/her name, last name, personal number (art. 26., par. 2 of the organic law), while information about party donations, including information containing a donor's name,

[5] SAO General Auditor Order of 5 August 2021, #012036/21

[33] SAO General Auditor Order of 7 February 2018, №01463/21

[34] The Rule approved by SAO General Auditor Order of 7 February 2018, №01463/21, article 4.8

last name and personal number is public (art. 26., par. 6). Accessibility of the said information is ensured by the SAO, according to the procedure prescribed by Georgian legislation. The SAO through its website should ensure public access to party donations on a monthly basis.

As noted earlier, SAO is also monitoring legitimacy and transparency of party financial activities. Within the scope of the monitoring, SAO may request full information about finances of natural or legal persons that have donated to the party, based on a court decision.

Clearly there is a legitimate basis for processing financial data of natural persons, however, in such cases, SAO should abide by the general rules for data protection, with regards to publication of already processed financial data or using other types of processing in relation to such data. During proceedings over illegal donations, name, last name and information about donations made can be processed for publication, which are open according to the law. In all other cases, financial data of such individuals should be protected.

As to proactive publication of information about donations (the following information on donations is published on the SAO website – in case of a natural person: name, last name, personal number, place of registration; in case of a legal person: name of the organization, identification number, legal address). When it comes to party donors, law provides for processing of their personal data, i.e., legal basis of processing exists – processing is provided for by law. It is however disputable whether there is a legitimate goal for making a personal number of a donor public. Processing of a personal number for identification purposes is a different issue. As to making such personal number public and ensuring its accessibility through a website, is needs to be defined more clearly if there is a legitimate goal for making such data public.

Openness of personal data of electoral subject candidates/electoral subjects

Notably, the Election Code contains norms regulating personal data. However, it needs to also be mentioned that the Election Code provides regulations for protection of personal data, while persons exercising a passive election right are subject to a different legal regime. This law provides definitions of an electoral subject and a candidate for electoral subject. A candidate for electoral subject is defined as a person nominated for registration in the respective election commission to run in elections; an electoral subject is defined as a party, an initiative group of voters, a candidate for member of public authority representative body, or a candidate for public official registered by the chairperson of an appropriate election commission.

GAC Chapter 3 concerns freedom of information. Pursuant to art. 44 of the Code, personal data of a nominee for an office shall be public. Further, for the purposes of GAC Chapter 3, an official

is defined as „an official defined under Article 2 of the Law of Georgia on Conflicts of Interest and Corruption in Public Institutions". Pursuant to this norm, elected officials – President of Georgia, MP, Mayor, Governor are officials, while pursuant to GAC Article 44, data submitted by nominees to an office is public. The list of officials provided in the law does not directly include a member of assembly (Sakrebulo), but it only refers to an assembly chairperson and his/her deputies, chairpersons of commissions and fractions and their deputies. However, the same legal approach needs to be applied to nominees for assembly membership (since pursuant to GAC Article 42, par. "f", everyone has the right to access all the information related to electing a person to an elective office). Further, pursuant to the Election Code of Georgia, „According to and for the purposes of this Law, the activities of the Electoral Administration of Georgia, electoral subjects, state authorities, and municipality bodies shall be open and public." [35]

Pursuant to the Election Code of Georgia, a candidate for electoral subject submits the following data: first and last name, date of birth (day, month, year), address (according to place of registration), personal number of a Georgian citizen, workplace (name of the institution, organization, enterprise, etc.), position (if unemployed, indicate „unemployed"), party affiliation (if no party affiliation, indicate „non-partisan"). A candidate should also submit information about his/her revenues. Information submitted by a candidate is verified. Failure to submit information or submission of incorrect information provides a basis for denying registration of the candidate.

Although the FOI Chapter of GAC does not contain a list of public data related to officials, the Election Code provides a list of public personal data that should apply to electoral subject candidates / electoral subjects. Therefore, the incorrect practice that exists with regards to accessibility of personal data of electoral subject candidates/electoral subjects should be changed. In addition, for SAO, which implements monitoring of financial activities of political associations of citizens, within the scope of its competencies established by the organic law of Georgia „the Election Code" and the organic law of Georgia „on Political Associations of Citizens", personal data of electoral subjects should also be accessible, as open and public information.

In practice, SAO has problems with regards to accessibility of electoral subjects'/candidates' **personal number, cell phone number and address**, while contact details are required in full for initiating communication with electoral subjects, for fulfilment of obligations established by law. As noted earlier, such standard is established by art. 57 of the organic law of Georgia „the Election Code of Georgia", according to which, if electoral subjects are violating requirements of law, **they should be warned in written by SAO and** should be required to correct the irregularity, and be provided with detailed information in writing about the violation in question). Notably, the CEC

[35] Organic Law of Georgia – the Election Code of Georgia, article 4

processes this data according to the requirements of the Election Code, however in practice the issue of transferring personal data of electoral subjects to SAO is problematic. The foregoing regulations clearly confirm that the existing practice should be changed. Additionally, a reference should be made to the Supreme Court practice. In many of its decisions, the Supreme Court has explained that **generally, status of a person affects the legal regime of data protection; in particular, the regime for public persons is different from that of other persons.** Protection of freedom of information is prioritized over protection of information about private life of public persons, as a person who wants to be a public person also declares readiness for possible interferences in his/her private life. **An official claiming that information in question concerns his/her private life is not proof that the information may not be accessed without his/her consent**. A person who actively participates in public life should accept that details of his/her private life may become a subject of public or media attention. The cassation chamber highlighted the fact that the requested **information concerned high-level officials, such as the Prime Minister of Georgia, the President, etc**. A person who actively participates in public life should accept that details of his/her private life may become a subject of public or media attention. This ensures certain openness of private life of political officials, accessibility of their personal data.[36]

Information containing a personal secret about an official may not be subject to an absolute protection, especially considering that an official, under the existing regulations, should expect that details of his/her private life may become an object of public interest, due to the fact that a person that makes decisions on behalf of the people should be a worthy representative of the people. Therefore, in the case in question, accessibility of personal data of officials serves a legitimate purpose – ensuring transparency of information about officials involved in electoral process.

Recommendation: since the Election Code does not contain a provision about openness of the afore-mentioned personal data of electoral subjects participating in elections (a reference is made to personal data required for registration) and the afore-mentioned legal conclusion is based on GAC Articles 42 and 44, as well as definition of terms in art. 2 of the Election Code, it is recommended that such provision be directly included in the organic law of Georgia – the Election Code of Georgia.

As to monitoring of parties by SAO during campaigning, in addition to regulations provided in the organic law of Georgia „the Election Code of Georgia", confirming that in view of objectives of the Election Code, activities of electoral subjects are open and public, another important document is the Regulation of transparency of political finances adopted by the SAO General

[36] Nugzar Skhirtladze, Legal aspects of personal data protection, p.67

Auditor[37], which prescribes rules of reporting for the purposes of monitoring of legitimacy and transparency of financial activities of persons with a declared electoral goal, electoral subject candidates and electoral subjects. Notably, SAO identifies potential violations by: verifying bank accounts opened for campaigning and submitted in relation to campaign financing; monitoring campaigning in media (including on social media); conducting field visits and accepting complaints.

The Constitution of Georgia recognizes that activities of political parties are based on the principles of their freedom, equality, transparency and internal party democracy.[38] Therefore, realization of equality of parties and the principle of equal elections is crucial during oversight activities of the Monitoring Department, which is ensured by observance of the high standard of transparency. In particular, all information related to reporting by electoral subjects as well as actions taken in response to possible violations should be accessible at any stage of the monitoring. This does not imply transfer of copies of internal documents, however, information about actions taken in response to violations by parties, electoral subject candidates should certainly be open and accessible for interested individuals. Further, what is prioritized here is not the „reputational harm" that a party/electoral subject may suffer but rather, activities of the monitoring authority based on the standard of transparent, equal approach, and support of such activities.

Therefore, SAO should improve the „Rule for provision of information about monitoring" available on its website, determining which type of information is provided at a particular monitoring stage, who provides this information and who is authorised to receive it. According to this Rule, proceedings at SAO consist of the following steps: preliminary assessment, closing (dismissing) a case after a preliminary assessment, or analysing circumstances of a case, not finding any violation, or finding a violation and preparing a report. After the proceedings are concluded, SAO publishes on its official website information about the subject of the proceedings and facts of the case. It also publishes information about a decision made by court. If the decision is appealed in a higher court, the information published on the website will be revised according to the decision made. **Information** about electoral subjects/candidates should be open for any interested individual (during preliminary assessment stage, after dismissing a case after a preliminary assessment, during further examination of a case or after finding of a violation). The issue of dismissing a case after a preliminary assessment should be especially transparent and corresponding reasoning and motivation should be provided **(this information should also be published on the website).**

[37] General Auditor order of 5 August 2021, #012036/21

[38] Constitution of Georgia, article 3.4

The existing approach (allows during a preliminary assessment access to information only on issues that have already been reported by media or if there is a risk of spreading mistaken information, which may mislead the public. In such an event, the Office may disclose information about the subject of the preliminary assessment and facts of the case. Further, when during a preliminary assessment, a media outlet learns about details of the case, the Office will provide information about results of the assessment to media outlets as well as to the subject of the assessment) should be changed and information about different stages of the proceedings should be accessible for all interested individuals.

Within the present study, we also analysed a decision of the State Inspector's Service, dated 31 December 2021, Nc-1/423/2021, which has not been appealed in court under the procedure prescribed by the Code of Administrative Offences. According to this decision, based on an application of a subject that participated as an independent candidate in local government elections, the Service reviewed a case concerning legitimacy of transfer/processing of personal data of administrative offenders by SAO, attached to a report of an administrative offence concerning failure to fulfil a legal obligation to submit campaign financial reports. In particular, judicial correspondence contained personal data of individuals (first and last name, personal number, phone number, address, as well as information on whether the electoral subject had been registered as a mayoral candidate or as a candidate for assembly membership (reference was made to the self-governing city and the municipality concerned), who were possibly subjects of administrative offence reports.

The State Inspector's Service found that in connection to accessibility of all information related to election of a person to an elected office, established by GAC Article 42 and personal data of officials and nominees for an office, provided in Article 44 of the same Code, the following should be taken into account: public access to information about an electoral subject, including to information about fulfilment/failure to fulfil legal obligation is an important component of accountability and financial transparency of electoral subjects. However, since for the purpose of financial transparency, openness and accountability of electoral subjects, the register of cases involving administrative offence is published on the SAO website after administrative proceedings are finalized in court, the State Inspector's Service found that in the case in question, correspondence sent by SAO to the court on 9 November 2021 (subjects of which also included other offenders) was related to the purpose of reviewing reports of administrative offence and were not related to publication of data for financial transparency of electoral subjects or their accountability before public. Therefore, the State Inspector's Service found that on 9 November 2011, SAO processed the data of the electoral subjects (independent candidates) referred to in Annex of an internal memo No014381/09 of 5 November 2021, in the form of transferring the data, without the legal basis provided in Article 5 of the law.

Clearly, the information about electoral subjects provided in the internal memo - first and last name, personal number, phone number, address, as well as information on whether the electoral subject had been registered as a mayoral candidate or as a candidate for assembly membership (reference was made to the self-governing city and the municipality concerned) - represents open information about officials/candidates, according to the law. While pursuant to art. 5, par. "b" of the Law of Georgia on Personal Data Protection, data may be processed if such processing is allowed by law.

In conclusion, the Political Finances Monitoring Department should take into account the following main points:

1. Everyone has the right to request access to information held at the monitoring department; access to public information may not be denied on grounds that an applicant has not provided a specific goal for requesting the information.
2. Access to public information must be ensured based on the principle of equality; all FOI applications should be handled within a reasonable period; if a request is denied, the monitoring department should provide reasoning within 3 days and specify relevant legal grounds.
3. The monitoring department should correctly determine cases when depersonalization of data is necessary, since personal data usually represent an integral part of information resources, while depersonalization of personal data ensures accessibility of a significant spectrum of information and confidentiality of personal data.
4. It is crucial that a denial of FOI request also includes the procedure and timeframe for appealing the denial. The monitoring department should not charge any fees for providing information, except for photocopying fees.
5. Internal documents are not **public information** and they are not accessible even to parties of administrative proceedings. An internal memo is an internal document and an administrative agency may not provide access to it, as public information.[39]
6. The monitoring department prepares a report of violation within the scope of its competences, the report is prepared within administrative proceedings and as a final product is referred to a court for further actions alongside materials of the proceedings. Given the standard of transparent monitoring of reporting by electoral subjects/candidates for electoral subjects, it is important to also maintain statistics of cases when proceedings were not initiated against such persons (case was dismissed after a preliminary assessment), with the aim of ensuring transparency of the process and

[39] Supreme Court of Georgia, case-589(k-19), of 25 November 2021

clearly demonstrating an equal approach of the department towards all electoral subjects.

7. Information about a preliminary assessment, closing of a case, further examination, conclusion of a case and preparation of a report of administrative offences, in relation to electoral subjects/candidates is accessible to everyone (not only after a court delivers its decision).
8. As to proceedings against natural persons that have made illegal donations, until court decision is made and the violation is found, accessibility of relevant information should be ensured by depersonalization of personal data.