ENSURING PERSONAL DATA PROTECTION IN CYBERSPACE

CHALLENGES AND NEEDS OF GEORGIA

The study was prepared by the Institute for the Development of Freedom of Information (IDFI). IDFI is responsible for the content of this material.

Author: Nata Goderdzishvili

Table of Contents

Introduction 4

Comparative Analysis of the European and Georgian Models of Personal Data Security in Cyberspace 5

Personal Data Cybersecurity in the European Legal System 5

Personal Data Cybersecurity in the Georgian Legal System 8

Serious Inconsistencies of the Georgian Law on Information Security with the NIS Directive 10

The Shortcomings of the Georgian Law on Information Security in Terms of Cybersecurity of Personal Dara 13

Summary 15

Recommendations 16

Introduction

The scale, frequency, and impact of cyber incidents are increasing on a daily basis, posing a major threat to the proper functioning of network and information systems and the integrity, accessibility, authenticity, and confidentiality of information transmitted/protected through technologies. Delays in the functioning of critical information systems and compromising information resources can significantly hinder or even bring the functioning of public or private organizations to a stop, cause significant financial losses, reduce consumer confidence, and cause great damage to the country's economy as well as to the normal functioning of civil society and civil turnover.

In the age of digital transformation, more and more online transactions are taking place and e-government or commercial services have a growing number of users. Consequently, most of the personal data today is accumulated in information systems, electronic registers, and communication networks. Thus, personal data is mostly breached by compromising these devices through massive cyberattacks resulting in violations of citizens' digital rights in cyberspace, including personal data. It should be noted that the protection of personal data is directly linked to the realization of the right to privacy, and ensuring the security of personal data in cyberspace in terms of absolute improvement influences the quality of our digital privacy/inviolability.

Cybersecurity is an additional guarantee for the protection of fundamental human rights and freedoms in the digital world, including for the realization of the right to privacy and the protection of personal data. The security of the digital environment is important not only for personal security, personal data protection, and privacy, but it also contributes to the dynamic development of the country and is an essential prerequisite for enhancing confidence in the economy, society, and democracy.

The security of personal data and privacy in the Internet space must be consistent and integrated into the cybersecurity framework and its practical operation. It is important to take a holistic, unified approach with regard to cybersecurity and personal data protection in the digital world and develop these issues in a mutually reinforcing rather than isolated and conflicting way. Integrating personal data protection into the cyber security management system can have a positive impact both in terms of strengthening cyber security and protecting personal data.

The purpose of this study is to examine the legal environment governing personal data protection and cybersecurity in cyberspace, to identify existing challenges and shortcomings, and to develop evidence-based recommendations based on the best European legal frameworks.

Comparative Analysis of the European and Georgian Models of Personal Data Security in Cyberspace

Personal Data Cybersecurity in the European Legal System

The secure operation of the digital market, efficiency and effectiveness of the digitalization process, a large-scale introduction of e-government and e-commerce services, as well as building the trust of the information society in new information solutions and the interest in using technological solutions largely depend on digital interconnectivity, cybersecurity, security, and resilience to risks and threats.

To this end, two parallel processes have taken place within the EU:

1) In 2016, the European Parliament adopted a directive on Security Network and Information ('the NIS ***Directive***') that aims to achieve **harmonized and uniform standards of cybersecurity** within the EU member states and to establish comprehensive safety norms and basic mandatory requirements at the horizontal level for the EU member states to ensure a high level of security of network and information systems so as to improve the functioning of the European internal digital market. The deadline for the transposition of the directive by EU member states was set to 2018.

The directive on Security Network and Information was specifically designed to regulate the security of network and information systems. **It aims to secure information systems, technological environment, computer infrastructure, integrity, authenticity, accessibility, and confidentiality of network and information systems in cyberspace.** Although the scope of the NIS Directive is not limited to ensuring personal data protection, the information and cyber policy, the legal, procedural, organizational, and technical norms of security that NIS Directive requires are largely similar to the data security approaches developed by both the EU General Data Protection Regulation (GDPR) and the international information security standards (ISO, NIST) and significantly contribute to the creation of a secure cyber environment for personal data processing and privacy.

2) A roughly similar process took place with regard to the Data Protection Framework Regulation (GDPR),[1] which was adopted by the European Parliament in 2016 as well, and since 2018 its implementation has become mandatory for member states. The regulation aims to protect the personal data of individuals and stipulates that **security is one of the main principles of personal data processing and a core obligation of the data controller as well.** In particular, data processing shall ensure protection from unauthorized or illegal processing, accidental loss, destruction, and damage. The regulation takes the protection of personal data to a higher level and intends to adequately protect the rights of individuals

[1] "Regulation 2016/679. 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)," accessed November 11, 2021, http://data.europa.eu/eli/reg/2016/679/oj

in the context of digital transformation and the introduction of new technologies. The regulation introduces new principles such as **accountability of the organizations that process the data, adopting risk-based methods and policies in data processing, the obligation to notify regarding the data breaches,** and more. In accordance with the regulation, the cybersecurity systems/services used to prevent, detect, and deal with cyber threats must meet European standards for the protection of personal data and privacy and, of course, the framework regulation.

While protecting personal data and data subject rights is the primary purpose of the GDPR, achieving this goal is impossible without the necessary technological and organizational measures that ensure a secure environment. The GDPR imposes a set of security obligations related to personal data protection, which is directly/indirectly reflected or must be reflected in the strategic and legal framework of cybersecurity.

Both legislative frameworks have individual perspectives and goals and stipulate adequate mechanisms for achieving them. Their areas of application also differ substantially: while the NIS Directive applies only to essential and digital service providers, the GDPR has a much broader scope: in addition to EU-registered organizations that in the course of its activities process personal data, it also applies to organizations outside the EU if they process the data of persons in the EU. If the NIS Directive is designed to protect all types of data in cyberspace, the GDPR only regulates personal data processing in all areas/mediums (automatic, semi-automatic, non-automatic).

According to the GDPR, data controllers have framework obligations regarding data security in order to ensure personal data protection, which includes both technical and organizational-procedural measures that directly or indirectly contribute to the strengthening of cybersecurity. In terms of cybersecurity, data controllers, for instance, are obliged to minimize data and limit the storage period, ensure confidentiality of the data, take security measures based on risk assessment, adhere to data protection standards when creating a new product or service (privacy by design), and ensure data protection by default (privacy by default), assess the effectiveness of security measures regularly, notify and deliver reports in case of data breaches, mitigate their potential adverse effects, ensure business continuity, and increase resilience.

The GDPR does not list specific security measures but requires data controllers to adopt relevant, appropriate, risk-based technical and organizational measures to protect personal data. The data controllers and data processors should evaluate existing circumstances, context, and conditions while taking into consideration the nature and purpose of the processing, determine the costs required for security measures, the probability/severity of the restriction/violation of data subjects' rights, and develop a data security policy. For instance, the GDPR recommends several technological solutions to ensure data security, such as pseudonymization and encryption of personal data and, in terms of organizational measures, the establishment of compliance certification mechanisms and internal security policies, testing and assessing the effectiveness of the measures regularly for secure processing of the data.

In a similar manner to that stipulated by GDPR, the NIS Directive states that in order to handle the challenges, risks, and threats to network and information systems security, **the Member States shall**

determine effective, customizable, compatible, proportionate, specific, verifiable, and inclusive technical and organizational measures to ensure the security of critical infrastructure (essential services and digital service providers). They shall take into account the following elements as well: the security of systems and facilities, incident handling, business continuity management, monitoring, auditing and testing, and compliance with international standards.

Analysis of the NIS Directive and the GDPR leaves one with the impression that these two frameworks were developed autonomously and completely independently of one another. Only a few articles of the NIS Directive indicate in a general manner that, when ensuring information and cyber security, the protection of privacy and communication and the protection of personal data must be in accordance with the requirements of the GDPR. Furthermore, only general provision regulates issues related to the cooperation and information exchange between the agency responsible for data protection and the competent cybersecurity authorities in the event of a personal data breach during a cyber-incident. As for the GDPR, the text of the regulation also contains a general provision that CERT / CSIRTs have a legitimate interest and grounds for data processing in order to ensure the security of network and information systems, prevent unauthorized access to them and malicious code distribution, and therefore protect personal data in such systems.

Although interrelated norms in these legal acts are scarce and featured in a general manner, this does not mean that there is no overlap between them in their practical applications. On the contrary, when networks and information systems are used to process personal data, in these cases, both the NIS Directive and the GDPR Regulation apply. For instance, if a personal data security breach occurs during a cyber-incident, an obligation arises to notify both the data protection agency and the competent authority for cybersecurity (CERT/CSIRTs). In addition, the incident may violate the requirements of both the NIS Directive and the GDPR, and finding an offense committed and imposing sanctions in accordance with both legal acts might be required.

It is challenging to answer an essential question such as the sufficiency of the security requirements set out in the context of the NIS Directive for personal data protection in cyberspace for the purposes of GDPR, since both legal acts are still new and European practice is currently being shaped by the cases of their implementation. While a positive answer to this question would completely prove the success of the European legal system, it might be advisable to analyse the NIS Directive security requirements for personal data protection in cyberspace on a case-by-case basis and identify flaws or compliance for each particular case.

Finally, it should be noted that the harmonization and consolidation of the personal data protection and cyber security legislative framework with European law is an obligation of Georgia under the Association Agenda and the Association Agreement with the EU. According to Annex I to the Association Agreement, Georgia is obligated to ensure compliance of personal data protection legislation with EU Directive 95/46 / EC, Council of Europe Convention 108 and its Additional Protocol, EU Framework Decision 2008/977/JHA of 27 November 2008, and Council of Europe Committee of Ministers Recommendation No.R(87)15 of 15 November 1987.

In terms of cyber security, in accordance with the Association Agenda between Georgia and the European Union, Georgia undertook the medium-term obligation (which should be achieved by 2022) to harmonize Georgian law on Information Security with EU Network and Information Security Directive 2016/1148 of 6 July 2016.

Personal Data Cybersecurity in the Georgian Legal System

In terms of personal data protection in cyberspace, the connection between the laws of Georgia on Information Security and Personal Data Protection is an important area for research.

Similar to the GDPR and NIS directive, Georgian legislation stipulates its area of application, goals, objectives, principles, competent authorities, and implementation methods in the context of cybersecurity and personal data protection.

The Georgian law on Information Security applies to the subjects of critical information systems, which, at this stage, are limited to public organizations, although, starting from January 1, 2022, it will also include the representatives of some private sector entities (presumably, energy, healthcare, financial, and banking sectors). On the other hand, the law on Personal Data Protection applies to all controllers processing personal data, both public and private entities and, in certain cases, controllers who are natural persons. Thus, for the moment, the scope of the Georgian law on Personal Data Protection is much broader than the Georgian law on Information Security. As for the object of protection, the purpose of the Georgian law on Information Security is to provide for the security, confidentiality, accessibility, and integrity of information and information systems in cyberspace. Information Security in cyberspace ensures the security of all kinds of information assets, including personal data. The protection object of the law on Personal Data Protection is the privacy and personal data of the data subject.

In a similar way to the GDPR, the Georgian Law on Personal Data Protection does not lay down specific measures but, in a general manner, requires implementation of appropriate technical and organizational measures adequate to the risks related to the processing (e.g., unauthorized or unlawful processing, accidental loss, destruction, or damage of data) by data controllers to ensure data security. The law also provides specific instructions related to logging/registering all data operations and strictly controlling the scope of the processing. The Georgian Law on Personal Data Protection is less adjusted to data processing in the cyber environment.

Despite its innovative approaches, the draft amendments to the Law of Georgia on Personal Data Protection prepared in 2019 and registered in the Parliament of Georgia are still general in terms of security of data processing, leaving wide scope for interpretation for all interested parties: the data subject, data processor, and even the oversight body. According to the draft law, when specifying the organizational and technical measures necessary to ensure data security, the controller and the processor must take into account the categories and volume of data, the purpose of data processing, form, means, and possible dangers of violating the rights of the data subject. Additionally, they shall periodically

evaluate the effectiveness of technical and organizational measures taken to ensure data security and, if necessary, ensure that adequate measures are taken to protect data security and/or update existing ones.

The draft amendments to the Law of Georgia on Personal Data Protection, prepared in 2019 and registered at the Parliament of Georgia, are progressive in terms of reporting actions compromising data and are in line with GDPR requirements as well. In particular, the data controller/processor is obligated to document an incident, its effects, the measures taken, and, no later than 72 hours after having become aware of the incident, notify the State Inspector's Service.

Interestingly, the law of Georgia on Personal Data Protection (article 17.5) refers to the Georgian legislation with regard to determining the measures for the protection of personal data. Although this reference in the norm is made with regard to the Georgian legislation in general and not to the Law of Georgia on Information Security specifically, given the scope of the latter, we should consider that the measures provided for by the Georgian law on Information Security apply in relation with the security of personal information contained/protected in networks and information systems in cyberspace.

In order to ensure data security, the Law of Georgia on Information Security lays out different organizational, procedural, and technological requirements for information and cybersecurity, such as taking an inventory of information assets to identify their criticality/sensitivity and establishing a management system (including access control system) for relevant categories (confidential, internal use, public), laying down the minimum information security requirements in an internal information security policy document, determining the authorized/delegated body at the institutional level, certifying authorized information and cyber security units, auditing information security on a periodic basis, carrying out penetration testing of the systems and services, an incident management system/an obligation to notify, and so on.

To sum up, when a data controller is at the same time a subject of a critical information system, it is essential that the personal data used in the information systems/services is unambiguously identified (including IP addresses, device identifiers, network log files, access control log files, and more) and, in order to protect and secure them, the principles of processing and security requirements (purpose limitation, storage limitation, privacy by design, privacy by default) provided for by the Georgian law on Personal Data Protection and also, security requirements (auditing security periodically, taking an inventory of information systems, access control) provided for by the Georgian law on Information Security are applied.

Serious Inconsistencies of the Georgian Law on Information Security with the NIS Directive

Georgia's striving for integration into the EU and the European Digital Single Market necessarily includes transposing the NIS Directive and the digital security requirements of the EU regulatory field, harmonizing with European standards and legislation.
In the course of analysing European approaches to cybersecurity, considerable emphasis should be placed on basic EU approaches to cybersecurity, such as:

The state should be focused on developing an approach of selecting a standardized, horizontal framework for regulating cybersecurity, introducing unifying requirements, rather than supporting fragmented, sectoral, chaotic solutions. EU cyber security regulation, above all, implies a unified cybersecurity approach for both its member states as well as the sectors subject to regulation.

For increasing resilience to cyber-attacks, the European model refuses to establish large-scale control over the activities of non-regulated sectors and involve supervisors at the operation level. Instead, the European approach is centered around critical information system subjects having opportunities for strong self-control, prevention, discretion, and the oversight bodies focusing more on solving strategic tasks while having fewer operational functions.

The European cybersecurity model requires having the separation of powers, checks and balances, and a clearly defined and predictable system of exercising the powers delegated to the cyber competent bodies.

Balancing the activities of competent cybersecurity authorities is achievable only with the aid of oversight mechanisms that are transparent, accountable, and open.

There are a number of inconsistencies identified[2] in terms of compliance of the Georgian law on Information Security with the NIS Directive. In this report, however, we are going to highlight some of the most important cases of non-compliance:

1) The governance framework has shortcomings, does not comply with any international model, and is tailored to the interests of certain authorized bodies. The complicated, chaotic, and ambiguous picture of information exchange, coordination, and cooperation, separation of competence areas, jurisdiction, and powers will inevitably lead to a conflict between powers, and furthermore, cases will arise where the identification of the responsible entity/person for a specific incident will be impossible.

Example 1: It is not determined how the sectoral oversight bodies exchange information and cooperate. Is there a national incident repository in the country at the national level, and who is responsible for

[2] "Cybersecurity Reform in Georgia: Existing challenges, International Practice and Recommendations | IDFI," August 2020, https://idfi.ge/public/upload/GG/CyberN333.pdf

managing it? Who is the delegated representative of the state (SPOC-Single Point of Contact)? Who makes the decision to mobilize or coordinate activities of the competent state bodies throughout large-scale cyber-attacks? Who is the responsible representative of Georgia in the international arena? Who makes attribution regarding the attacks on Georgia by state actors? Etc.

Example 2: According to the legislation, the National Bank of Georgia, as a supervisory body for the financial/banking sector, serves a quasi-regulatory function in cyberspace. If this model is the rule rather than the exception, then what role, as sectoral supervisors, do the Georgian National Energy and Water Supply Regulatory Commission (GNERC) and the Communications Regulatory Commission have in terms of cybersecurity?

2) The lack of a comprehensive state approach to cybersecurity (whole-of-nation principle).

Furthermore, the connection between the legislative framework and the national strategic framework is ambiguous.

The supervisory bodies impose sectoral information and cybersecurity requirements on different categories of critical infrastructure subjects, such as the rules for auditing, classifying incidents, and so on. As long as there is a lack of coordination of the work and more-or-less standard information and cybersecurity requirements are not established in the process of drafting subordinate acts, we will end up with different regimes and practices. At a time when the EU obligates the member states not only to take a harmonized approach between sectors, but also introduce a common strategic, operational, and procedural framework between countries.

According to the NIS Directive, the strategic and legislative frameworks of countries shall be developed and enforced in a cooperative and interrelated manner. Both the NIS Directive and the new EU draft proposal (NIS 2) on updating it indicate explicitly, at the very least, what issues need to be covered by the strategy.

The Georgian Law on Information Security does not mention cybersecurity strategy and its essential elements. It is noteworthy that the National Cyber Security Strategy, as the central political document expressing the unified vision and will of the government, was approved after a three-year delay only after the amendments to the above-mentioned law were approved.[3] However, the new strategy also failed to involve the institutional and organizational governance model. The problem of consistency and coherence between the law and the strategy is exacerbated by the current situation, as the law is one of the mechanisms for determining strategic visions, goals, and objectives, and, taking into consideration the absence of a governance model in the strategy, approving the new amendments to the law of Georgia on Information security leaves a number of serious issues unclear.

3) **The danger of producing a mixed picture or results about cybersecurity in the country** with the current model of attributing critical information system subjects to the relevant supervisory bodies and imposing different sectoral standards/requirements.

[3] "The ordinance №482 of the Government of Georgia on the Approval of the National Cyber Security Strategy of Georgia 2021 - 2024 and its Action Plan," September 2021, https://matsne.gov.ge/document/view/5263611?publication=0

According to the NIS Directive, critical information system subjects shall be identified not by their legal form (either private or public legal entity) but by their sectoral affiliation.[4] In addition, the supervisory regime is harmonized and not sectorally circumscribed.

For instance: the regime established for the subject of the first category will apply if the GNERC becomes the target of a cyber-attack, and it will be subject to the regulation of the Operational Technical Agency (OTA) under the State Security Service. In a similar way, the supervisory requirements of the Digital Governance Agency will apply to an energy company (e.g., Telasi), and if a state is a shareholder of an energy company (e.g., State Electrosystem), the OTA regime will apply to it as well. Such a framework of governance poses the risk to the timely exchange of information and of weakening sectoral cyber resistance even in one specific sector.
Imposing different requirements and enforcement mechanisms according to the categories will, of course, lead to different outcomes between sectors in terms of the introduction of information and cybersecurity. Therefore, the efficiency and success of the activities of supervisory bodies will also vary in proportion to the mechanisms of their control and monitoring. And most importantly, all this will have an impact on creating a sustainable, unified, and predictable cybersecurity environment in the country, which is the main objective of the Georgian Law on Information Security.

4) Excessive control and supervision regime

The supervisory model provided for by the Law of Georgia on Information Security, instead of focusing on cyber-resistance and self-strengthening of critical infrastructures, often allows the supervisory body to hold the reins and directly interfere in operational activities. The supervision regime of supervisory bodies is limited to day-to-day operative level, activities of accessing and controlling the critical information systems. In the case of NIS, the main focus is on supporting and strengthening the subject, not on managing cyber-attacks instead. The NIS Directive is centered on balanced and proportionate technical and organizational measures. Therefore, the principles of proportionality, balance, and necessity must also be observed under the mandate of supervisory bodies.

5) The lack of a risk management approach

The amended Law on Information Security, as well as the previous version, did not provide for and, even now, the risk-based approach is not provided for in the case of the management of information assets or when implementing information and cybersecurity policy. At the same time, both the NIS directive and the new EU NIS2 proposal consider the process of risk-based management and decision-making a major cornerstone of information security management systems.

[4] The NIS Directive stipulates horizontal criteria for determining operators for essential providers (degree of damage/loss when compromising the information system, market share, geographical area of spread, the number of users) and allows for determining sector-specific factors as well.

The Shortcomings of the Georgian Law on Information Security in Terms of Cybersecurity of Personal Dara

The Georgian law on Information Security has nothing to say about the protection of privacy and personal data. The law does not require supervisory entities or critical information systems subject to adopt appropriate personal data protection measures/effective mechanisms when they have access to data or are otherwise processing it.

1) Network Monitoring System

The Georgian law on Information Security raises questions about a potential personal data protection breach in relation to network sensors. Considering its characteristics - accessibility, the network sensor is a sensitive technology, since its deployment creates a high risk of breaching the rules of personal data processing. Therefore, the rules for configuring a network sensor shall provide all the necessary guarantees to ensure that all data processing rules are duly followed when using sensor devices.

On the one hand, the definition of article 2 of the Georgian law of Information Security implies that the purpose of network sensors is not accessing the information stored or transmitted through the system, but rather it is designed for detecting computer incidents against information systems. This interpretation is further supported by article 4, para. 4, which stipulates that *the Operative Technical Agency, the Digital Governance Agency, and the Data Exchange Agency shall have no access to the information or information assets of a critical information system subject (except in cases provided for in this law).* On the other hand, it is fair to note that the provision of the law, which says that *network sensor shall not allow for access to the content of communication,* does not provide a legal guarantee for avoiding any misuse of network sensors once installed or ensuring that it is not possible to have access to personal information. In addition, defining the network sensor configuration rules through a subordinate law in the future leaves these issues unanswered.

These issues should be regulated by unambiguous and clear norms codified in the law instead of regulating them under the umbrella of subordinate laws that need to be developed in the future on the basis of the law already adopted. It is important to note that the rules set out in subordinate laws can be changed frequently, easily, and unpredictably, with fewer opportunities for detailed analysis and criticism by outsiders. Furthermore, the existence of an independent and impartial body with supervisory functions over the operation of the network monitoring system is crucially important.

2) Obligation to notify after the personal data is compromised

Personal data is often compromised as a result of cyber incidents. Therefore, the Operational-Technical Agency and the Digital Governance Agency, as well as other competent cyber security bodies provided for by law, must cooperate with the State Inspector's Service to avoid personal data breaches in cyberspace and exchange information timely and efficiently regarding the personal data breach resulting from a cyber-incident and work together to minimize serious effects and mitigate harm.

According to the GDPR, for example, in the case of a personal data breach, the controller shall, not later than 72 hours after having become aware of the breach, notify the supervisory authority and the persons affected by the incident. However, if a personal data breach is followed by a cyber-incident, the notification shall be made in accordance with the procedures set out in the NIS Directive. The controllers must record all cases of data security breaches and the measures taken. They are also responsible for developing data security policies, plans for incident detection, and responses.

The Law of Georgia on Information Security does not provide for such regulations in cases of a personal data breach during cyber incidents and, generally, does not determine other forms of information exchange and cooperation with the State Inspector's Service.

Further, the NIS Directive emphasizes that notifying CERT / CSIRTs of incidents by critical entities may require the processing of personal information and that such processing shall be in line with the requirements of the GDPR and the ePrivacy Directive. The information exchanged shall be limited to data that is relevant and proportionate in relation to the purposes for which they are exchanged. The information confidentiality, the security of the controllers, and commercial interests must be protected when such an exchange of information takes place. Also, the Georgian law on Information Security does not contain a provision about notifying CERT / CSIRTs with regard to a cyber incident.

3) **Ensuring the rule of law, adhering to the principles of purpose limitation, proportionality, and necessity** when requesting information (including personal data) from critical information system subjects and obtaining access to information.

A number of provisions of the Georgian law on Information Security provide the Operational-Technical Agency, the Digital Governance Agency, and the Cyber Security Bureau with guarantees to have direct access to information assets in their supervisory sectors and request information in a mandatory fashion. For instance: they are authorized to obtain not only information security policy with relevant internal rules, but also any other information related to the development, implementation, monitoring, and improvement of information security policy from critical information system subjects, and after processing, to issue mandatory instructions. Although having access while exercising supervisory powers is not new to both the current NIS Directive and the NIS2 Directive proposal designed for its improvement, these powers do not exist without proper safeguards for control and oversight. In particular, Article 15 (2) of the NIS Directive stipulates that "When requesting such information or evidence, the competent authority shall state the purpose of the request and specify what information is required." All such provisions should comply with the requirements of the EU Charter of Fundamental Rights, including the principles of effective judicial protection, proportionality, and individual assessment of the circumstances of a case. Such a regime applies to all types of supervision mechanisms and enforcement measures in cyberspace.

Under the mandate granted to OTA by the Georgian law on Information Security, the risk of unjustified access to information assets of the first (public institutions) and second category (telecommunication

companies) subjects and processing of protected information is higher, as the law authorized OTA to have, without the permission of the courts, direct access to information systems of public entities and any representative of the telecommunications sector and indirect access to personal and otherwise sensitive information stored in the systems.
Prescribing procedural or legal protocols by the law is crucial, and if they are met, it can be considered that the request for access by the supervisory body is substantiated, and only then can access be granted. Otherwise, with only a general statement by OTA that there is a threat and it requires access, the subjects of the first category will be obligated to comply with the request immediately.

4) **Clear and established frameworks of oversight mechanisms and monitoring for cases of abuse of power** by competent cybersecurity agencies.

The law does not provide for specific guarantees and procedures and leaves open the issue of the mechanisms for control and oversight of the powers of OTA. With regard to exercising delegated powers in the fields of information and cybersecurity, all existing and possible supervision mechanisms (Parliamentary, judicial, prosecutorial, supervision by the state inspector, internal audit, or other possible mechanisms) that can apply to OTA need to be studied and analysed in detail in order to ensure close and effective supervision of it. It is also noteworthy that merely incorporating the referral norms on this or that supervisory mandate into the law does not solve the problem. Rather, all the procedural, organizational, or technical guarantees must be prescribed that will reasonably and unequivocally make OTA an object of control and oversight, leaving the latter with no legal or other means to abuse or misuse its power and engage in any other illegal activity under the mandate of information security.

Summary

In Georgia, throughout the past decade, the standards of cybersecurity and protection of personal data have significantly developed at the level of both legislative and practical implementation. The organizational-institutional framework has been established in both fields, knowledge of specialists working in these areas increased, appropriate strategic and legislative frameworks have been created, which, along with the regulation, should create favorable environmental conditions for cyber security and personal data protection development.

Although cybersecurity and personal data protection standards have been developed, given the global challenges, the dynamics of cybersecurity and protection of personal data, there are still many challenges in these areas, in both private and public structures. A clear example to illustrate this is the report on the

activities of the State Inspector's Service 2020, according to which breaches related to data security measures increased by 10% compared to 2019.[5]

Georgia, which is a country with European legal culture and is in the process of European integration, should continue to intensify its efforts to harmonize domestic legislation with European regulatory standards. The introduction of European standards of cybersecurity and personal data protection will be another step forward for Georgia to integrate into the European digital single market, while, in the course of personal data processing, the citizens of Georgia will be provided with a high standard of security in cyberspace and mechanisms for effective and efficient protection of human rights and freedoms, including the privacy.

Recommendations

● The Georgian law on Information Security should clearly stipulate **the avenues of cooperation between competent cybersecurity authorities and the State Inspectors' Service** in matters related to personal data protection, including personal data security breach or/and a cyber incident. **The protocol and legal procedure for the exchange of information** should be established. Strengthening competent authorities with so-called tabletop exercises and relevant training courses is crucial for proper planning of the notification process with regard to the personal data breach related to the incident.

● The Georgian Law on Information Security should have **precise and definite rules/criteria for determining critical information systems subjects,** which may be supplemented by sectoral characteristics. More clarity at the legislative level will leave authorities with less space for subjective discretion and give sectors greater opportunities for sustainability and foresight. Many EU countries, including Estonia, have a well-established practice of determining critical sectors at a legislative level.

● The Georgian legal system (The Georgian law on Information Security or the Law of Georgia on Personal Data Protection) should list specific organizational and technical measures, their purpose (e.g., ensuring integrity, accessibility, and confidentiality of the data), or determine precise requirements (e.g., using certified systems, developing internal data protection policy documents - internal rules), the introduction of which ensures the security of personal data.

● It is crucial to carry out an in-depth analysis of whether the Georgian Law on Information Security, in terms of data security in cyberspace, complies with the requirements of the Georgian law on Personal Data Protection, and based on the analysis, **at least for critical information systems subjects, it will be clearly identified what standards should be followed to ensure the security of personal data in cyberspace.** In particular, whether the introduction of ISO 27001, the minimum information security requirements, and the cybersecurity services are sufficient for protecting personal data in cyberspace.

[5] Brief Overview of Recent Developments in the Field of Personal Data Protection | IDFI, May 2021, https://bit.ly/3oEGcn8

● Since the Georgian Laws on Personal Data Protection and Information Security, despite the differences in their objectives and area of application, have significant legal and practical overlap in terms of the protection of personal data in cyberspace, it is advisable to bring the activities of the competent bodies in these areas closer, **cooperate more intensively, and take measures in a coordinated manner.** At the initial stage, the central areas for cooperation are: directing specific areas of auditing in a coordinated manner, giving information security and cybersecurity specialists and personal data protection staff training on overarching issues, raising their knowledge, and exchanging information.