PERSONAL DATA
PROTECTION SERVICE

JOURNAL OF PERSONAL DATA PROTECTION LAW

N2, 2023

Journal of Personal Data Protection Law

№2, 2023

The second issue of the Journal of Personal Data Protection Law
is dedicated to the 10th anniversary of the Georgian Personal Data Protection Supervisory Authority

P-ISSN 2720-8745
E-ISSN 2720-8761

Table of Contents

From the Editor-in-Chief

The following issue of the Journal of Personal Data Protection law is dedicated to the ten-year anniversary of the establishment of the Georgian Personal Data Protection Supervisory Authority.

The Personal Data Protection Service welcomes this remarkable date with a number of innovations.

On June 20, 2023, by the decision of the the “European Data Protection Board” (EDPB), the Personal Data Protection Service obtained the Status of Observer to the Board’s activities. The “European Data Protection Board”, as an EU body, is established on the basis of the “General Data Protection Regulation” (GDPR) and consists of representatives of the Data Protection Supervisory Authorities of each EU member state, the European Commission and the “European Data Protection Supervisor” (EDPS). It plays an essential role in ensuring the effective enforcement of personal data protection regulations across the EU, establishing consistent, uniform, and best practices for data protection supervisory authorities.

The Board based its decision to grant observer status to the Personal Data Protection Service of Georgia on several criteria: Activity and degree of independence of the Service, legal regulations and the commitment declared by the state — the international obligation taken for the purpose of joining the European Union to fully comply national data protection legislation in accordance with the rules applicable in the European Union. Also, it should be noted that the Board consulted with the European Commission and various institutions of the European Union to achieve homogeneity.

This decision is of utmost importance, signifying that the Personal Data Protection Service of Georgia is now a respected member of the European community of the data protection authorities, which, on one hand, marks a significant achievement for us, while on the other hand, it entails an enormous responsibility, of which every employee of the service is keenly aware.

On June 14, 2023, a new Law of Georgia "On Personal Data Protection" was adopted to strengthen the Personal Data Protection Service of Georgia on the way to European integration and to ensure a high standard of the right to data protection in the country, which marks a crucial step forward in the development of personal data protection law in Georgia. The adoption of the law was driven by the necessity to align existing legislation on personal data protection with European standards, to fulfill Georgia’s international obligations, and the need to establish internationally recognized principles and best practices.

It is crucial to harmonize personal data protection legislation with EU regulations and subsequently integrate new standards at the national level.

The new Law of Georgia "On Personal Data Protection" proposes such important changes as refining existing terminology or establishing completely new concepts in the field of personal data protection.

The law redefines the term "data subject consent", "audio monitoring", broadens the definition of "direct marketing", introduces such an important new term as "profiling". In addition, one of the important issues is "pseudonymization" of data.

In addition to terminological innovations, the new law defines the "transparency" of data processing at the level of principle. The mentioned principle holds great importance for the data subject in terms of the protection and realization of their rights. It must be clear and transparent to the natural person that their data is being processed or planned to be processed. The principle of transparency requires that data subjects have access to information regarding the processing of their personal data.

The new law expands the data subject's rights and establishes guarantees for the protection of mentioned rights. One of the new rights that the new law gives to data subjects is right to transfer data, the so-called right to data “portability”. The right to data portability will make it easier for data subjects to use certain services. In turn, it is important for companies to ensure the implementation of appropriate technical facilities to enable the transfer of personal data from one information technology environment to another and, most importantly, to implement appropriate security measures during the process.

The impact assessment mechanism on data protection provided by the new law is of great importance, which is a novelty for the Georgian legislation on personal data protection and considering the rapid development of new technologies, it aims to reduce the increased threats of human rights violations.

The new law "On Personal Data Protection" reframes issues related to direct marketing. It is noteworthy that according to the new law, regardless of the basis of data collection or extraction and their availability, data processing for direct marketing purposes will be possible only with the consent of the data subject, unlike the current norm. In addition to the name, surname, address, telephone number, and email address of the data subject, processing other data for direct marketing purposes will require the written consent of the data subject. It should also be noted that before obtaining the consent of the data subject and during the implementation of direct marketing, data controller/data processor must explain to the data subject in a clear, simple and understandable language their right to withdraw consent at any time, along with the mechanism and rules for using this right.

Among the n provided by the new law, an important requirement is the appointment of a personal data protection officer in public and some private institutions.

According to the law, the data protection officer ensures:

- Informing the data controller, data processor and their employees on issues related to data protection, providing them with consultation and methodical assistance;
- Participation in the development of the internal regulations related to data processing and the impact assessment document on data protection, as well as monitoring the implementation of Georgian legislation and internal organizational documents by the data controller or data processor;
- Analyzing the received statements and complaints regarding data processing and making relevant recommendations;
- Receiving consultations from the Personal Data Protection Service of Georgia, representing data controller and data processor in relations with the Service;
- In the case of the data subject's request, to provide them with information about data processing stages and their rights;
- Additionally, the data controller or data processor undertake other functions with the aim of enhancing the standards of data processing.

The obligation to appoint or designate the officer applies to public institutions, insurance organizations, commercial banks, microfinance organizations, credit bureaus, electronic communication companies, airlines, airports, medical institutions, as well as individuals acting as data controllers and data processors, who process the data of a large number of data subjects or engage in systematic and large-scale monitoring of their behavior. Furthermore, the normative act of the President of the Personal Sata Protection Service of Georgia determines the circle of persons who are not obligated to appoint or designate a personal data protection officer.

Although the law imposes the obligation to appoint an officer only in the case of the individuals listed above, other data controllers, however, at their own discretion, have the right to appoint or designate a personal data protection officer. According to the law, the personal data protection officer must possess proper knowledge in the field of data protection. In addition, data controller and data processor are required to provide the officer with appropriate resources and independence in the process of carrying out activities. Furthermore, they have an obligation to proactively publish the officer's identity and contact information on the website (if applicable) or through other available means.

The establishment of the data protection officer institute is of particular importance as it brings the Georgian personal data protection legislation closer to European standards and significantly strengthens the guarantees of protecting the rights of data subjects. It can be asserted with certainty that the actual implementation of the data protection officer institution will have a substantial preventive effect and qualitatively contribute to strengthening the legality of the data processing process.

One of the issues that is changing significantly involves administrative fines. The new law imposes a warning or a fine for the violation of any obligation or rule defined by the law "On Personal Data Protection". For example, a data controller may be held liable for breaching data processing principles or grounds, or for bypassing direct marketing requests, unlawfully conducting audio or video monitoring, not having a data protection officer when required by the law, etc.

The new law also broadens the scope of administrative responsibility for offenses and enhances the measures of responsibility.

Similar to the current law, the new legislation still specifies fixed fine amounts, although these amounts have been significantly increased. Specifically, the fine amount was tied to the offender's organizational structure and annual turnover. For instance, a violation of any of the principles of data processing stipulated by the law will result in a warning or a fine of 1,000 GEL for an individual, public institution, non-entrepreneurial (non-commercial) legal entity, as well as a legal entity, a branch of a foreign enterprise and an individual entrepreneur whose annual turnover does not exceed 500,000 GEL. Engaging in the same action by a legal entity (except for a non-entrepreneurial (non-commercial) legal entity), a branch of a foreign enterprise, and an individual entrepreneur whose annual turnover exceeds 500,000 GEL will result in a warning or a fine of 2,000 GEL.

A novelty in the law includes the definition of mitigating and aggravating circumstances. Furthermore, failing to comply with the legal requirements of the Personal Data Protection Service of Georgia is deemed an administrative offense, for which the amount of the stipulated fine is 1000-2000 GEL. The mentioned change will contribute to the effective implementation of the decisions made by the Service and will have a significant impact on the improvement of the overall situation of personal data protection in the country.

It is important to note that the statute of limitations for administrative offenses under the new law has been increased to 4 months instead of the existing 3 months, which can also be considered as an important preventive and a facilitative measure for effective supervision.

Under the new law, if, during data processing considering new technologies, data categories, volume, purposes, and means of data processing, there is a high probability of a threat to the violation of basic human rights and freedoms, the data controller is obliged to conduct an impact assessment on data protection in advance.

In cases where, following the impact assessment, a high threats of violating basic human rights and freedoms is identified, the data controller is obligated to take all necessary measures to substantially reduce these threats. Additionally, if necessary, the data controller is entitled to contact the Personal Data Protection Service for consultation. It should be noted that if it is impossible to substantially reduce the threat of violating basic human rights and

freedoms with additional organizational and technical measures, data processing should not be conducted.

According to the new law, there is an obligation to report a data breach to a supervisory authority when the incident poses a significant threat to basic human rights and freedoms. Additionally, should be noted that, according to the new law, the criteria for determining an incident that poses a significant threat to basic human rights and freedoms, as well as the procedure for reporting this incident to the Personal Data Protection Service of Georgia, should be specified by the normative act of the President of the Service. Furthermore, the new law mandates informing the data subject about the incident.

The main provisions of the new law of Georgia “On Personal Data Protection” will take effect from March 1, 2024, while the institution of the data protection officer, the obligation to assess the impact on data protection and the regulations governing administrative offenses related to them will come into force from June 1, 2024.

The implementation of the new law will significantly enhance the personal data processing stages. On the one hand, it will reduce the cases of law violations, thereby strengthening the preventive effect, on the other hand, it will empower the Personal Data Protection Service of Georgia for more effective supervision and response.

We serve the implementation of the European idea, values and principles of personal data protection in Georgia!

Prof. Dr. Dr. Lela Janashvili

President of the Personal Data Protection Service of Georgia
Professor at Ivane Javakhishvili Tbilisi State University
Visiting Professor at the Autonomous University of Barcelona

Levan Ioseliani

Welcome Letter

Dear Reader,

It is my pleasure to address you through the Journal of Personal Data Protection Law. As the Public Defender of Georgia, I warmly welcome and express my positive appraisal for the initiative of the Personal Data Protection Service of Georgia to launch a legal journal in this field.

In the age of modern technology and digital transformation, where progress takes on various forms daily whether it is computer programs, social networks, applications, or artificial intelligence — steadily encroaching into our personal space, initiating live discussions on the legal aspects of personal data processing and establishing an additional forum provides specialists in the field and representatives of scientific circles with a valuable opportunity to engage in discussions about the protection of personal life and data.

This necessity is also prompted by the fact that not too long ago, the primary European data protection regulation came into force and in Georgia, a new legal regulation was adopted at the national level. The current circumstances emphasize the heightened importance of consistently organizing academic discussions and dialogues on personal data protection issues in Georgia, which is crucial for the continued development of this legal field.

Simultaneously, it is noteworthy that the Public Defender has been actively pointing out in the parliamentary reports in recent years that in terms of access to public information in the country, the closure of open information containing personal data content and disregarding existing public interests for transparency has become a big challenge, which poses difficulties both for the people who want to receive public information, as well as for public institutions, for the effective management of their activities. In the country, given the provisions of the Georgian Law "On Personal Data Protection" and the presence of a supervisory institution on personal data protection, there is a discernible imbalance between the right to access public information and the mechanisms for safeguarding the right to privacy. Moreover, as per the Public Defender's assessment, such negative practices primarily stem from the misinterpretation of the Georgian Law "On Personal Data Protection" by the data controllers. For instance, state institutions decline to disclose information containing personal data, citing the absence of consent from the relevant subject as the basis for refusal. It disregards the fact that the legislation acknowledges alternative grounds for furnishing such information, which are entirely unrelated to the consent of the data subject.

I believe that the periodic publication of the scientific journal on personal data protection and the inclusion of problematic issues or academic evaluations within it will prove highly beneficial for the appropriate development of practice.

Once again, I express my gratitude to the Personal Data Protection Service of Georgia for this initiative, I am confident that such a scientific publication will contribute to the effective protection of rights, the advancement of this legal field, and the enhancement of awareness about it. It will also serve as a valuable forum for scientific discussion.

Levan Ioseliani

Public Defender of Georgia

Leonardo Cervera Navas

Welcome Letter

Dear Reader,

It is with great honour that I welcome you to the second issue of the Journal of Personal Data Protection Law, a great academic initiative of the Georgian Data Protection Authority, aiming at contributing to and enriching the educational sources in the field of data protection, as well as cultivating a data protection culture.

Our era is characterised by rapid and ever-evolving technological developments and digitalisation, which in turn entails an unprecedented increase in the processing of personal data. Both the opportunities and the risks that come with such advances are important, and they each deserve consideration on their own merits.

The present day, therefore, dictates an imperative need for data protection authorities to deepen their understanding of practical legal challenges in the field of privacy and data protection on the one hand, and, on the other hand, raise and reinforce public awareness around those topics. Initiatives like the Journal of Personal Data Protection Law, bringing together academics, legal practitioners and individuals interested in law and fundamental rights, in particular these of privacy and data protection, present a great opportunity to achieve both objectives, and fulfil the tasks that the General Data Protection Regulation (GDPR) vests in data protection authorities.

Following a promising first issue, where topics such as data subjects' rights under the GDPR, transparency, the role of Data Protection Officers and Artificial Intelligence were analysed, I am confident that this Journal will continue providing a platform for discussion that manages to surpass the geographical borders of Georgia.

I invite you to enjoy this issue and I hope that it inspires you.

Kind regards,

Leonardo Cervera Navas

Secretary-General of the European Data Protection Supervisor

Norbert Bernsdorff*

"Data Protection Law" of the European Union**

1. Data Protection and the European Commission's Requirements of 17 June 2022

I would like to start my presentation with a question: Does the European Commission – EU Commission - complain about deficits in Georgian data protection at all? If so, are they substantial or does the existing data protection law just need a "fine-tuning"?

The opinion of the EU Commission of 17 June 2022 is ambivalent: The Commission demands - firstly - "to equip the...Personal Data Protection Service with resources to its mandate" and - secondly - "to ensure its institutional independence" (page 17). Elsewhere in her report (page 10), she states that "the Personal Data Protection Service...still needs to prove its efficiency and independence". That is all the opinion contains.

In my first presentation I already referred to the so-called Copenhagen criteria that an applicant country must fulfil. One of these criteria is the "acquis criterion" – from the French word "acquis communautaire". According to this, a candidate state must adopt the entire body of rules and regulations of the European Union (EU), meaning integrate several 10,000 pages of legal texts into its national law and implement them into corresponding administrative and judicial structures. What the "acquis" comprises in the area of European data protection law results from the "Association Agreement" between the EU and Georgia from 2014. There, in an "Annex" (I and XV-b) to Article 14 and Article 327 of the "Agreement", reference is made to data protection law of the Council of Europe and now obsolete - no longer valid - law of the EU... one more reason to look at the current, completely redesigned legal situation in the EU today.

2. Adoption, Implementation, Enforcemen

First of all, a question of understanding needs to be clarified: If a candidate country has to adopt the EU rulebook, how is this done technically?

The EU has no legal means to carry out the integration of its law into the national law of the candidate state itself. Like accession, this is done voluntarily by the candidate country. There are three stages in the integration of EU law: "adoption", "implementation" and "enforcement", meaning "law enforcement". For the first two stages, the terms "transposition", meaning "conversion of law", and "application", meaning "application of law" are also commonly used. The integration of EU law into national law is regularly an apolitical process. There will be fewer so-called "veto players" here; because political disputes in the candidate state have already taken place before, namely before the application for membership was submitted.

What does the term "compliance" mean in this context?

---

* Professor at Philipps University of Marburg (Germany); Retired Judge at the Federal Social Court of Germany.

** The publication represent the text of the report presented by the author within the framework of public lectures held in the scope of cooperation of Ivane Javakhishvili Tbilisi State University Law Faculty and Institute of Administrative Sciences. The event was dedicated to the issues of Georgia's integration with the European Union.

"Compliance" or "non-compliance" refers to the phase after accession to the EU. It refers to whether a member state complies with the adopted law of the EU completely or not at all, only incompletely or late. This is monitored by the EU Commission and the Court of Justice of the EU (CJEU). The keyword here is: Infringement proceedings!

Is the integration of EU law at the first level - "adoption" or "transposition" - an automatic process?

Yes! - The technical instrument for this is the "accession" of the candidate country. This takes place through the accession agreement (under international law) with all other EU member states. From the date of accession, the candidate country becomes a party to all treaties of the EU in their current version. All EU legislation concluded on the basis of these treaties up to the date of accession automatically becomes binding on the acceding state. The EU legislation take precedence over any national law. This is explicitly recognised by the candidate country in the accession agreement (under international law).

What does this mean for EU data protection law? - With accession, this also "grows" into the national legal order as a priority right!

In this lecture, I do not want to compare Georgian and European data protection law with each other; my aim is not to look for successes or deficits of a future "adoption" or "transposition". I cannot do that at all, because I do not have the so-called progress reports, the "Association Implementation Reports" which have been produced annually since 2016. These are held by the EU Commission and the competent authorities in Georgia; however, I am neither an employee of the EU nor an official representative of the member state Germany. To make such a comparison is the task of TAIEX, the "Technical Assistance and Information Exchange" Group of the EU Commission, which should have been in Georgia since last year.

So what is my task today?

I want to give an overview of

- firstly: the so-called primary law and the so-called secondary law of the EU, here above all the General Data Protection Regulation.
- secondly: current areas of conflict under data protection law in the EU
- thirdly: new legal developments and
- fourthly: the requirements of European law for effective data protection control.

3. The European Union's Primary Data Protection Law

All EU action is based on the European treaties. These treaties between EU member states set out objectives and rules for the EU's institutions as well as the decision-making processes and the relationship between the EU and its member states. The treaties are the basis for EU law and are referred to as "primary law" in the EU. The legislation based on the principles and objectives of these treaties is called "secondary law" and includes regulations, directives, decisions, recommendations and opinions.

a. Primary and Secondary Law

Since 2009, when the Lisbon Treaty came into force, the legal framework for data protection in European primary law has been the Charter of Fundamental Rights of the European Union – European Charter of Fundamental Rights, in this case Article 8. Although the primary law level also includes Article 8 of the European Convention on Human Rights and a Council of

Europe Convention from 1981, the focus of my presentation will be on Article 8 of the European Charter of Fundamental Rights.

In order not to let my lecture get out of hand, I will also limit myself to the presentation of secondary data protection law. Although there is now a wealth of secondary law regulations and directives in the EU, I will focus here only on the General Data Protection Regulation, which has been in force since 2018. It is now the central legal institution for the protection of personal data in Europe and has led to a radical change in data protection law in the EU.

b. Article 7 and Article 8 of the European Charter of Fundamental Rights

The protection of personal data is an essential aspect of the protection of private life. The latter is regulated in Article 7 of the European Charter of Fundamental Rights. Because it considered it so important, the EU has dedicated a separate, special provision to data protection - in this different from the European Convention on Human Rights - namely Article 8. The fundamental right to data protection must be respected by EU institutions, bodies and agencies, as well as by each EU member state when implementing European law.

What does "implementation of EU law" mean in this context?

First of all, it should be noted that EU member states are not bound by EU fundamental rights if they exclusively apply their national law; then national fundamental rights apply. The case is different when EU law - for example a European directive - is implemented. This also happens through national "legal acts" of the EU member states; however, these are only "interposed" and ultimately represent an "extension" of EU sovereignty. National courts have to apply European fundamental rights in addition to national ones. This sounds complicated, but when thought through, it is simple.

c. Essential Baselines

I do not want to keep you long with dogmatic subtleties. Therefore, only a few hints at this point:

Article 8 of the European Charter of Fundamental Rights is an enforceable right. Like any classical fundamental right, it is above all a right of defence against the state and its authorities. However, Article 8 also obliges to ensure the protection of personal data by private parties. The fundamental right to data protection thus has a so-called third-party effect.

In the area of data protection, Article 8 of the European Charter of Fundamental Rights contains statements on the scope of protection and on when an interference with the right to protection of personal data is justified; furthermore, Article 8 requires the establishment of "independent bodies" to monitor compliance with data protection law. Whether the holders of fundamental rights also include legal entities has not yet been clarified in the EU.

The fundamental right to data protection has a special feature - and this is the last thing I will say here: It is "reverse engineered"! - In German it is referred to as "norm-engineered".

What does that mean? - It means that the fundamental right to data protection is predetermined at all levels by the respective current European secondary law - in this case the General Data Protection Regulation. The content of Article 8, which is part of the primary law of the EU, is therefore derived "one-to-one" from the content of the secondary law, which is at a

normative level lower. If secondary law changes, the fundamental right also changes. This is a result that is actually not compatible with the principle of the so-called hierarchy of norms.

What is the EU's motive behind this?

The development in the field of processing personal data is very dynamic. The intention was to make the fundamental right to data protection "open to the future". Secondary law can be adapted to such processes more quickly and easily than primary law.

4. Secondary Law: General Data Protection Regulation

Since May 2018, the General Data Protection Regulation – abbreviated GDPR - has been in force at secondary law level. It replaced a European directive that had existed since 1995, the so-called Data Protection Directive (95/46/EC).

a. The Differences Between an EU Regulation and an EU Directive

What impact this has on European data protection only becomes clear when one knows the differences between an EU regulation and an EU directive:

Directives are limited to prescribing a certain result for EU member states. The achievement of this result, on the other hand, is left to the member states themselves; they have to transpose directives within certain deadlines through their own national legal acts. In contrast, EU regulations are directly and immediately binding on all EU member states and not, like a directive, only with regard to a result to be achieved.

What prompted the EU to replace the former Data Protection Directive with a Regulation?

With the former Data Protection Directive, all EU member states had the same legal basis. However, they could determine the implementation of data protection themselves.

Accordingly, there was a considerable imbalance in the level of data protection in the individual EU member states. With the introduction of the GDPR, which is directly and immediately binding on all member states, this imbalance should be eliminated.

At this point, one more remark! - Because the fundamental right to data protection in Article 8 is being filled out by the secondary-law GDPR - I have just reported on this - the Regulation is being elevated to the rank of a fundamental right, so to speak. However, this is disputed in European legal dogmatics.

b. Principles and Key Points of the General Data Protection Regulation

I would now like to familiarize you with some of the central contents of the GDPR. I do not claim to be exhaustive. Nevertheless, it should become clear what level of data protection the EU has been aiming for since May 2018.

(1) On the One Hand: No Limitation of Data Protection to Risky Information Processes

The GDPR does not limit its application only to risky information processes such as "profiling", "scoring" or the use of so-called "artificial intelligence". Rather, it applies universally. And rightly so; because ubiquitous computing has paved the way for "big data" at all levels. Data power in the hands of the state and in the hands of private individuals is growing. Individuals,

however, are supposed to retain control over their own data and thus the ability to exclude third parties from collecting or using this data. They should be able to obtain information about the collection of their personal data and to work towards the deletion of data. Because personal data is now collected everywhere, such data must be protected not only in critical areas but also in everyday life.

(2) On the Other Hand: No "Brake Block" for Economic Development

Recently, the data protection commissioner of a federal state in Germany resigned from his service. He belongs to the "Free Democratic Party (FDP)" in Germany, which primarily represents business and economic interests. The reason he gave was: The European data protection is anti-business. It puts the EU economies at a disadvantage in the international competition. Data protection fails to recognize that personal data also has an economic potential, an economic value.

A widespread prejudice must be cleared up here! - The GDPR does not prohibit the use of personal data in the economy, it actually protects it. Article 1 of the GDPR explicitly safeguards the "free movement of personal data". This may therefore neither be restricted nor completely prohibited for reasons of data protection. Data processing in the economy is therefore not taboo; it only has to comply with the processing conditions regulated in Article 6 of the GDPR. To ensure that European data protection does not “stifle” digitalization in the economy - file-based and “artificial intelligence” applications - supervisory authorities and courts in the EU have an important task: They must not overemphasize data protection or even "make it absolute", but rather must appropriately balance the interests of the economy against the protection of personal data.

Current example: Because it considers data protection to be absolute in this way, the European Court of Justice prohibits the use of software for video conferencing systems if it comes from outside Europe - in this specific case, the USA: Zoom, Microsoft Teams, Cisco Webex etc. But, as long as there are no corresponding technical alternatives in Europe, the European economy needs them.

(3) Scope of Application — Establishment Principle, Market Place Principle, Data Transfer to Third Countries

The situations to which the GDPR applies are governed by Article 2 of the Regulation. In principle, this applicability is comprehensive; the GDPR is binding for both public and non-public bodies, meaning also for private parties. However, it does not apply to police activities and law enforcement. A separate directive applies here, but it is structured similarly.

The GDPR presupposes automated data processing. This is to be understood broadly; Article 2 is "technology-neutral" in this respect. This does not include purely analogue storage of data and purely manual data processing – on index cards, paper forms, etc. Exceptionally, the handling of personal data in the family sphere is not covered by the GDPR. This is called the household privilege.

Does the GDPR apply only in the EU or worldwide because of the global flow of data across all borders?

In our networked world, the processing of personal data hardly knows any technical boundaries. Therefore, the application of the GDPR must be geographically limited. Because all

member states of the EU are obliged to provide the same level of data protection, it naturally applies geographically without restriction in the EU. However, particular caution is required in the case of data processing by non-European companies; data transfers to countries outside the EU also give rise to suspicion. The level of data protection is often significantly lower there. The GDPR solves these problems in Article 3 with the so-called establishment principle and the so-called market place principle. Non-European Companies with an establishment in the EU are bound by the Regulation, but a mere letterbox in the EU is not sufficient for this. If such a company does not have an establishment in the EU, it is nevertheless bound by the GDPR if it operates in the internal market of the EU. Therefore, Google and Facebook – Meta - are subject to European data protection law.

What about personal data in the cloud? Is there a "loophole" here? – No! - In such a case, it depends on where the server is located.

If data is exported to third countries, an adequate level of protection must be provided there. That of the EU - often referred to as the "data protection gold standard" - is frequently not achieved. According to Article 45 of the GDPR, such a data transfer must be allowed by the EU Commission in a so-called adequacy decision. I will come to the data protection agreements with the USA later.

(4) General Prohibition with Reservation of Permission, Legal Permissions and Consent

To the European data protection law, the following basic principle applies: The starting point is a general prohibition with a reservation of permission.

What does this mean? - The processing of personal data is generally prohibited unless it is permitted by law or the owner of the data - the "data subject" - gives his or her prior consent. The EU has thus agreed on a preventive approach that gives high priority on the protection of personal data.

Article 6 of the GDPR regulates when the processing of personal data is legally permitted. I do not want to go into too much depth here; therefore, only very briefly! There are five grounds for permission: Data processing is lawful when it concerns the conclusion or fulfilment of contracts; after the contractual relationship has ended, however, personal data must be deleted again. A data processing may also take place if a vital interest of the "data subject" is affected, for example in the fight against epidemics - Corona - or natural disasters. Processing is also permitted in the case of a legitimate interest of the person processing the data. This is the case if the "data subject" is his customer in business transactions or is employed by him; such a legitimate interest is, for example, the prevention of fraud by the "data subject". Finally, the performance of public tasks is sufficient for data processing. The European case law on this is now almost unmanageable.

As an alternative to legal authorizations, the prior consent of the "data subject" may justify the processing of personal data. Here too, just a few remarks: Consent must be voluntary, and the "data subject" concerned must know the meaning of his or her consent. Minors up to the age of 14 cannot give effective consent as a rule. Subsequent consent to the data processing - called "authorization" in legal terminology - is not sufficient to justify it.

(5) The Classification of data

Personal data can be classified. Some data can be obtained from generally accessible sources - from telephone and address books, from the internet, others have to be obtained in a complicated way. Some data are important for the integrity of a person - they are sensitive, others are not. In most cases, generally accessible and less sensitive data are less essential from the perspective of the "data subject". Because Article 6 of the GDPR does not differentiate here, Article 9 of the Regulation contains stronger protection for qualified data. This includes, for example, data on ethnic origins, political and religious beliefs, health and sexual orientations.

What does European data protection provide for so-called public figures - politicians, judges, actors, etc.?

There is a strong public interest in persons who are prominent, that is to say who have a certain degree of notoriety. Within the so-called public sphere - in the case of public appearances or public statements - the data protection of these persons is restricted. In this sphere, personal data may be collected, for example photos may be taken, without their consent. If this area is left and it concerns the so-called private or even intimate sphere - domestic sphere and family - the same protection exists as for unknown persons.

Article 9 of the GDPR then applies without restrictions.

(6) Information Duties, Rights of Access, Rectification, Deletion and Blocking

As a novelty compared to the previous legal situation, the GDPR provides for numerous rights for data holders in Articles 12 to 17. They are intended to help enforce the right of defense under data protection law. This begins with the duty of information of a processor of personal data who in this way must "open" the "black box" of his processing. This also applies above all in cases of a "data breach", when data flow in an uncontrolled manner. Protection instruments that require the "data subjects" to take the initiative themselves are a right of access and a right of rectification against the processor of the data.

Particularly noteworthy is the right of the "data subject" to have his or her data deleted in Aricle 17 of the GDPR. This has made a name for itself in recent years as the "right to be forgotten". The European Court of Justice has clarified this right in four decisions against Google since 2014. If personal data are not deleted, they can be blocked for users.

(7) Data Protection "in Advance": Data protection "By Design" and "By Default"

Let me now address one last point:

A ground-breaking innovation of European data protection law is also that it wants to take preventive action and prevent breaches of data protection "in advance". Until now, the only legal instruments available in this area were the regulations on so-called data economy or data minimization. Now, the sparing use of personal data is to be supported through technical or organizational precautions - "data protection by design" - or default settings - "data protection by default". The first area includes, for example, so-called pseudonymisations, the second area so-called patterns. Violations of these principles are punishable by fines.

c. Excursus: Law of Georgia on Personal Data Protection

As part of my preparations, I only looked very briefly and superficially at the Law of Georgia on Personal Data Protection, which I found on the homepage of the "Personal Data Protection Service". I assume that this is still valid. From the latest amendments to the law in December 2016 it appears that the former European Data Protection Directive (95/46/EC) still served as a model for this. However, as just discussed, the GDPR is now setting new priorities. Two things struck me: On the one hand, the Georgian law largely exempts the media from the application of data protection law when they collect data for journalistic purposes.

On the other hand, the law - as I read it - is also applicable to analogue data processing - "processing of data by non-automatic means".

5. Current Areas of Conflict in the European Union

As I have already stated in my presentation, the right to protection of personal data is not a "super fundamental right". It is not granted completely without limits or conditions. For example, it can collide with the - also protected - right of internet users and media companies to obtain information. But it can also come into conflict with the freedom of art, science and research. This is then called a "multipolar conflict". In these cases, the different interests must be weighed against each other and balanced: so-called practical concordance.

a. Data Protection and Freedom of Information - Internet Users and Media Companies

There is always an emotional debate in the EU about the relationship between data protection law and freedom of information; the latter is a manifestation of freedom of expression. Why this is so, is easily explained: The "data subject" wants to retain control over his or her personal data. As a rule, internet users and media companies usually want to invade privacy as much as possible.

Question: Does the GDPR contain a solution to this conflict?

Yes! - However, the EU does not balance these conflicting interests itself. Instead, Article 85 of the GDPR assigns this task to the EU member states. They must enact legal provisions for this purpose. Article 85 is a so-called opening clause, which gives the member states a "margin of appreciation". However, the GDPR does give one instruction: Paragraph 2 of the aforementioned provision obliges the member states to regulate "derogations" and "exemptions" from the GDPR if the data processing serves journalistic purposes. Background: Such a "media privilege" was and still is widespread in the national law of the EU member states.

Just for interest: What measures by the member states can be considered here?

One instrument, for example, is to oblige platform operators to set up filter systems - so-called upload filters. However, an upload filter system that is too far-reaching and lacks contours, with the consequence of "over blocking" even content that is not problematic from a data protection perspective, is likely to violate freedom of information.

b. The Permanent Problem of "Data Retention"

The issue currently attracting the most media attention is the so-called data retention. This refers to the obligation of telecommunication companies to store location and traffic data of

users of their services without concrete reason and over a long period of time. The aim is to make it easier for the security authorities to fight serious crime and international terrorism.

The so-called data retention has already written legal history: Originally, a European directive had required EU member states to store location and traffic data "in advance". After initial reluctance on the part of the European Court of Justice, the directive was declared invalid in 2014. The reason: The directive disproportionately restricted the protection of personal data.

In the following period, the European Court of Justice reviewed national laws on so-called data retention. In doing so, it has remained true to its original line, according to which such a retention represents a disproportionate encroachment on data protection law. Nevertheless, the EU member states have repeatedly enacted regulations on so-called data retention. In total, the European Court of Justice has handed down seven rulings against Germany, Estonia, France, Ireland, Austria and Sweden in the last ten years. In the political arena, alternatives to so-called data retention are now being discussed: the so-called login trap and a so-called "quick freeze" procedure. The so-called login trap allows the automated storage of the IP addresses of criminals without technical leading to a mass surveillance. With the so-called "Quick Freeze" procedure security authorities can have location and traffic data "frozen" at the provider. They can then access it with a court order.

c. Application of So-called Artificial Intelligence: ChatGPT

The use of so-called artificial intelligence is in principle not a subject of regulation under the GDPR. Nevertheless, it can pose problems in terms of data protection law.

One example is the text robot "ChatGPT"; "GPT" stands for "Generative Pre-Trained Transformer". It has been on the market since November 2022 and is currently attracting a lot of attention worldwide. In order to classify it in terms of data protection law, one needs to know something about how it works: "ChatGPT" is supposed to generate texts based on user input. It is based on so-called artificial intelligence that has been trained with a huge amount of data. It is true that individual users can protect their personal data by not entering it into the tool. However, the main data protection problem lies elsewhere; it concerns the text robot's database. There is a risk that the training material also contains data with a personal reference. In case of doubt, their processing can lead to a "data breach" for which the user is held responsible. The fines of the GDPR are high.

d. Transfer of Personal Data to the USA

I have already mentioned that cross-border data traffic with third countries - for business and trade - is necessary, but risky for data protection. According to Article 45 of the GDPR, such a data transfer requires a so-called adequacy decision by the EU Commission. This also applies to the transfer of personal data to the USA.

Since the "Edward Snowden" case and his surveillance by the US intelligence service, trust in American data protection in the EU has been – more or less - lost. EU citizens can also be observed in the USA, for example when they send messages via the US network Facebook - Meta.

In 2000, the EU Commission concluded a data protection agreement with the USA, called "Safe Harbour". It regulated compliance with data protection principles to which American companies had to commit. This was intended to "raise" the level of data protection in the USA

to that in Europe. Five years later, the European Court of Justice declared this "Safe Harbour" agreement invalid. The Court referred to the USA PATRIOT Act, which allowed American security authorities to access personal data without the consent of the "data subject".

In the following years, a new agreement was negotiated with the USA, the "EU-US Privacy Shield" agreement. Although it provided for improvements in data protection, it was still not sufficient for the European Court of Justice. In 2020, the Court also found this - and the EU Commission's so-called adequacy decision - to be unlawful. What this means is clear: It is currently still illegal under data protection law to transfer certain personal data from the EU to the USA. For information, the EU Commission is currently in the process of drafting a third EU-US data protection agreement.

6. The Future Development of the Data Protetion Law – Regulatory Frenzy of the European Commission

I now want to say a few words about legal developments in the EU!

Data is everywhere and increasing at a breathtaking pace. The hereby associated benefits for business, science and administration are euphorically welcomed. Data has become a key advantage for the economy. At the same time, the disadvantages for the protection of personal data resulting from a free flow of data are lamented. Both views are sometimes irreconcilably opposed to each other. However, there is agreement that Europe needs a legal framework beyond the GDPR.

Since 2020, the EU Commission has been working on a so-called European strategy for data; with this, it wants to enforce a single market for data that is as free as possible in the interest of the EU's economies and its global competitiveness. To this end, it has made proposals for four European regulations: With the first, a "Data Governance Act", it wants to create "data intermediation service providers", who, as neutral bodies and without economic self-interest, collect data and, if certain legal requirements are met, distribute it to interested parties. This principle is called "data altruism". In this way, it wants to limit the power of data monopolists such as Apple, Amazon, Facebook – Meta – and Google. The second proposal for a "Data Act" goes even further: It should regulate who owns the data that users of networked devices – such as surveillance systems or autonomous vehicles - generate themselves. So far, only the providers of such systems can access them, but not the users.

But the EU Commission is not leaving it at that!

It is also planning a "Digital Services Act". This aims to regulate online platforms; it is aimed at internet providers, cloud services, app stores and social media. Such companies must take measures to detect and remove illegal products and content at an early stage. Violations face fines of up to 6 percent of annual turnover. Finally, a "Digital Markets Act" is in preparation. It targets only the big "gatekeepers": Apple, Amazon, Facebook - Meta, Google and Microsoft. According to this, providers of messenger services and social media are to be obliged to offer so-called interoperable services. A WhatsApp message should then also be received via "Threemo-Messenger" and "Signal". Companies like Apple also have to grant access to other app stores. I don't want to go into this further here. Some of these regulations have already come into force.

Because data protectionists no longer know where "up and down" is in the digital jungle from all the initiatives of the EU Commission, they are calling for new, more effective instruments of data protection. One of the instruments is the creation of a "data ownership regime". As with the ownership of property, this should regulate who has the authority to

dispose over and to use personal data. Comparisons are drawn with copyright law. Should people be able to sell and transfer their data? - Another objective is pursued by the “Charter of Fundamental Digital Rights of the European Union" proposed by data protection experts. It is intended to supplement the European Charter of Fundamental Rights, here Article 8, and to protect personal data even better through specialized fundamental rights. A revolutionary concept!

7. Data Protection Control – “Data Protection Law Compliance” and External Supervisory Authorities

Effective data protection needs monitoring. No right can be effective if there is no monitoring of whether it is respected. The right to protection of personal data is particularly sensitive because individual violations often go unnoticed. A data protection control must take this into account.

How is this issue dealt with in EU law?

If one looks at primary law, that is to say Article 8 of the European Charter of Fundamental Rights, it hardly provides any answers. It is true that paragraph 3 of the fundamental right to data protection requires the establishment of "independent bodies" to monitor obedience to the protection of personal data. However, the legal meaning of this requirement is disputed in the EU. Only a few experts see it as a genuine institutional guarantee.

The GDPR is more detailed here. It is "two-track" and systematically distinguishes between "internal control" and "external control". According to this, the task of monitoring is initially assigned to the processors of data, the authorities and companies. According to Article 37 of the GDPR, they are obliged to appoint a data protection officer. He or she is independent within the authorities or companies. It is true that the data protection officer does not have to be involved in the leading decisions of the authorities` or companies` policies; however, he or she has free access to every processing operation and is to be involved in decisions on this. It is interesting to note that such an obligation for "data protection compliance" did not exist under the law of the Data Protection Directive (95/46/EC) in force until 2018.

Could European law leave it at this mere self-regulation?

The answer is: No! - It is true that internal control by such data protection officers makes sense; for they know the processes in and the structure of their authorities or companies well and can therefore carry out systematic and regular controls effectively. However, such internal controls are often also characterized by hierarchies and dependency relationships. For this reason, the GDPR also relies on a concept of "external control" by external data protection supervisory authorities.

What do one need to know about this "external control" at the level of the EU member states? - I will only briefly outline the system of data protection supervision in the GDPR:

According to Article 51 of the GDPR, independent supervisory authorities are to be provided for. "Independent" means "completely independent". The European Court of Justice understands this to mean that the data protection supervisory authority has to be remote from the government, meaning the supervisory authority must not be subordinate to a ministry. Excluded from the supervisory activities are - because of the "media privilege" - the media, also the churches and, according to Article 55 of the GDPR, the courts. Background: This is to ensure the independence of the judiciary. The main task of the data protection authorities is classical supervisory activity with the possibility of imposing fines of up to 10 million euros. The

supervisory authorities are also appeal bodies. Appeals against their decisions can be lodged with the courts.

To conclude my presentation, the following anecdote: It is well known that there is a massive "control deficit" in data protection law in all EU member states. Recently, someone calculated that companies in Germany therefore only have to expect a review by the data protection authority every 200 years (!).

Gergely Barabás[*]

Evolution and Revolution of Supervisory Authority Powers in Hungary with Special Regard to the GDPR

GDPR is a game changer in European data protection law. It has brought revolutionary changes, the fundamental and complete transformation of the role of supervisory authorities, their proceedings and relationship with the judiciary. GDPR has radically raised privacy-awareness across organisations of any kind and it is a radical breakthrough in data subjects', data controllers' and the courts' beliefs and behaviours with regard to the importance of data protection.

Hungarian data protection law has also come a long way, with a number of substantive, procedural and organisational changes. Nevertheless, the tendencies are clearly moving in one direction: due to the brutal growth of the data-based economy and services, the protection of personal data requires strong and effective powers. The development of data protection law in Hungary has already directed the organisational and procedural legal framework to an administrative-type model by establishing a more and more effective toolbox of corrective powers even before the GDPR. As regards the role of administrative justice in this process, the administrative judiciary in Hungary more and more actively claims a decisive role in the interpretation of data protection law. This process is far from over, on the contrary we are at the very beginning. The subject of this paper is to present the changes that have taken place in Hungary over the past 30 years, with special regard to the impact of the unified European data protection regulation. The analysis goes through the significant stages of data protection law and shows how the GDPR has generated developments in the powers of the supervisory authority.

Keywords: *Data protection, Administrative authority, Supervisory authority, Administrative justice, Judicial review, GDPR, Corrective powers, Data protection administrative procedure at the request of the data subject, Data protection administrative procedure ex officio, Temporary corrective powers.*

[*] Legal Counsel, Head of Department of Legal Counsels, Hungarian National Authority for Data Protection and Freedom of Information.

"*They can keep track of what I phoned and when, why, and to whom.*
They write in files what I dreamed of, and also, who understands it.
And I can't guess when there'll be enough reason to look up the file
which violates my rights. […]
My leader controls me from within! We are humans, not beasts --
we are minds! Our hearts, while we desire, not data in a file.
Come, freedom! You give birth to an order for me,
educate with nice words, but let it play too,
your handsome, serious son!"

József Attila[**] / "I can't breathe" / 1935

1. Introduction

The National Authority for Data Protection and Freedom of Information (hereinafter "the Authority" or "the NAIH") in Hungary is responsible for monitoring and promoting the enforcement of two fundamental rights: the right to the protection of personal data and the right to freedom of information (access to data of public interest and data accessible on public interest grounds). The Authority is also authorised to launch a procedure for the supervision of classified information in order to establish whether classification is lawful.

Based on constitutional provision, the Act CXII of 2011 on the right to informational self-determination and on the freedom of information (hereinafter "the Act CXII of 2011"), which entered into force on 1 January 2012, established the Authority and regulated its operation in detail. From an organisational perspective, the NAIH is an autonomous state administration organ; it shall not be instructed in its functions and shall operate independently of other organs and of undue influence. The tasks of the NAIH shall only be determined by an Act of Parliament.

However, regarding the organisational and procedural landscape this has not been always the case.

The first general data protection act (Act LXIII of 1992 on the Protection of Personal Data[1] and Public Access to Data of Public Interest[2]; hereinafter "the Act LXIII of 1992) in Hungary – as one of the cornerstones of the rule of law – entered into force in 1993 after the change of regime.

[**] 1 April 1905 – 3 December 1937 – József Attila was one of the most famous Hungarian poets of the 20th century. Generally, not recognized during his lifetime, József become the best known of the modern Hungarian poets internationally.

[1] Article 2(1): 1. 'personal data' shall mean any data relating to a specific (identified or identifiable) natural person (hereinafter referred to as 'data subject') as well as any conclusion with respect to the data subject which can be inferred from such data. In the course of data processing such data shall be considered to remain personal as long as their relation to the data subject can be restored. An identifiable person is in particular one who can be identified, directly or indirectly, by reference to his name, identification code or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

[2] Article 2(4) 'data of public interest' shall mean any information or knowledge, not falling under the definition of personal data, processed by an organ or person performing a state or local government function or other public function determined by a rule of law, or any information or knowledge pertaining to the activities thereof, recorded in any way or any form, irrespective of the manner it is processed and its independent or collected character.

The Act LXIII of 1992 had the following rules relating to judicial enforcement of data protection rights.

In case of infringement of his rights the data subject may institute court proceedings against the data controller.[3] The burden of proof that the data processing has been in compliance with the pertaining rules of law shall lie with the data controller.[4] The data controller shall be liable for any damage suffered by data subjects as a result of an unlawful processing of their data or as a result of an infringement of the technical requirements of data protection. The data controller shall also be liable for any damage suffered by the data subject resulting from the actions of a technical data processor. The data controller shall be exempted from liability if he proves that the damage was the result of force majeure beyond the sphere of data processing.[5] No compensation shall be paid for the part of damage suffered by the damaged person as a result of his intentional or grossly negligent conduct.[6]

The rules set out in Articles 17-18 provided for the litigation(s) between the data subject and the data controller fell within the jurisdiction of the civil courts.

However, the other pillar of judicial protection was almost completely missing from the Hungarian data protection system for a long time: the judicial review[7]. This was primarily due to the fact that the Data Protection Commissioner which was established by the Act LXIII of 1992[8] did not act as an administrative authority, its powers were '*soft*', that is, the Commissioner did not issue legally binding administrative decisions due to its legal status, and as a result its legal positions as administrative decisions "ruling" on the lawfulness of processing operations could not be brought before the administrative judge. On the other hand, according to the theory of data protection law in Hungary which reflected in the substantive text of the law, processing operations belonging to public administration did not qualify as an administrative activity or act the assessment of the lawfulness of which would have been subject to judicial review. The lawsuit brought before court by the data subject in relation to processing operations of administrative bodies had been considered as civil law litigations.

The result of this overall regulatory concept established by the Act LXIII of 1992 was that the legal interpretation issues related to protection of personal data *almost completely* avoided the administrative courtrooms for about two decades. The "case-law" developed by the Data Protection Commissioner could thus evolve over a long period of time by means of "*soft law*" without either the data subjects or the controllers having been able to challenge the compliance of processing operations with the law before administrative courts.

The Fundamental Law of Hungary[9] and the Act CXII of 2011 by establishing expressly the Authority as an administrative authority[10], transferred the protection of personal data to the

[3] Article 17(1).
[4] Article 17(2).
[5] Article 18(1).
[6] Article 18(2).
[7] Judicial review is a type of court proceeding in which a judge reviews the lawfulness of a decision or action made by a public body.
[8] Article 23(1) In order to safeguard the constitutional right to the protection of personal data and to public access to data of public interest, Parliament shall elect a Data Protection Commissioner from among Hungarian citizens with a university degree, a clean criminal record and an outstanding academic knowledge or at least 10 years of professional practice, who have significant experience either in conducting or supervising proceedings involving data protection or in the scientific theory thereof.
[9] The Fundamental Law of Hungary (25 April 2011).
[10] Article VI of the Fundamental Law of Hungary (1) Everyone shall have the right to have his or her private and family life, home, communications and good reputation respected. Exercising the right to freedom of expression

competence of a supervisory public authority and embedded it more strongly into the public sphere[11]. The judicial review of the decisions of public authorities is a constitutional requirement in all States based on the rule of law.

The establishment of the Authority and the enforceability of the protection of personal data through public powers have created a fundamentally new situation for the administrative judiciary, as well. This is the case even if it is factually true that the Act LXIII of 1992 had already given in 2004 the Data Protection Commissioner a toolbox of public powers[12] which, in terms of its legal status, would probably have strengthened its role as a public authority.

2. Enforcement of the Act LXIII of 1992 (1993-2012)

2.1. The Beginnings

As I have already noted, during this period data protection law issues *almost completely* avoided the administrative judiciary courtrooms.

It cannot be stated that the provisions of the Act LXIII of 1992 were completely unknown to administrative judges. The reference to the rules of this Act was indeed part of the administrative litigations in other groups of cases, although, as mentioned above, the reference to data protection infringements appeared rather as an auxiliary feature in lawsuits against administrative decisions – for example in tax and competition cases. The administrative judges dealing with tax, competition or other administrative cases did not consider it to be evident that, in the case brought before them, whether directly or indirectly, it was for them to interpret the rules of the Act LXIII of 1992 and to rule on their correct interpretation in order to assess the legality of a different type of administrative act.

2.2. Relationship Between Data Protection and Other Fields of Law

and assembly shall not impair the private and family life and home of others. (2) The State shall provide legal protection for the tranquillity of homes. (3) Everyone shall have the right to the protection of his or her personal data, as well as to access and disseminate data of public interest. (4) The enforcement of the right to personal data protection and the right of access to data of public interest shall be monitored by an independent authority established by a cardinal Act.

[11] Section 38 (1) -(2) of the Act CXII Section (1) The Authority shall be an autonomous state administration organ. (2) The Authority shall be responsible for monitoring and promoting the implementation of the right to personal data protection and the right of access to data of public interest and data accessible on public interest grounds, as well as for promoting the free movement of personal data within the European Union.

[12] Article 25(4) -(5) of the Act LXIII of 1992 (4) If the data controller or technical data processor fails to discontinue the unlawful processing (technical processing) of personal data, the Data Protection Commissioner may order in a decision the blocking, deletion or destruction of unlawfully processed data, prohibit the unlawful processing or technical processing of data, and suspend the transfer of data to foreign countries. The decision may not be remedied in administrative way. (5) The data controller, the technical data processor or the data subject may request judicial review from the court against the decision of the Data Protection Commissioner pursuant to paragraph (4) – within 30 days after its receipt – on the grounds of infringement. The Court shall proceed according to the regulations on lawsuits against public administration of the Civil Procedure Act. Until a final court decision, the data concerned may not be deleted or destroyed; the processing of data, however, shall be suspended and the data shall be blocked.

An illustrative example of the above-mentioned practice is the tax case in which the administrative court did not examine the lawfulness of the tax authority's processing operation in spite of the applicant's express claim, simply on the basis of lack of competence. The applicant complained that, on the basis of a letter of assignment, the tax authority was authorised by law only to collect data relating to the undertaking during the course of the tax investigation, but the tax authority went beyond that scope and made extra-enquiries among the applicant's private bank accounts, private vehicles and real estate. According to the applicant, the tax authority infringed the rules of the Act LXIII of 1992 and he objected as a data subject to the processing of his personal data by the tax authority. He also stated that he did not intend to lodge a separate data protection procedure against the tax authority.

The answer of the administrative court *was the following: "[p]ursuant to Section 16/A[13], the administrative court has no jurisdiction in relation to the processing of personal data. If the data subject, in this case the applicant, objects to the processing of his or her personal data, the controller – the tax authority – has to decide on this. If the data subject does not agree with the decision, he/she may apply to a civil court of general jurisdiction. In the absence of its own jurisdiction, the administrative court could not deal with the data protection objection on the merits in the tax case.'[14]* In this judicial argument, the strange is not what it records, but what it does not. It simply failed to argue why the court did not consider it possible to review the tax authority's decision on that basis. The action complained not only about the right to object, but also a breach of more general data protection provisions. This judicial argument sought to separate the role of the administrative authority as an authority from that of a controller.

The above-mentioned administrative judicial attitude is even more clearly illustrated by a judgement in which the Hungarian Supreme Court did not deal with the aspect of data protection law and its impact on the tax matter. It argues that *"[t]he Civil Code and the Act LXIII of 1992 to which the applicant made reference, do not contain any rules for resolving the tax dispute, and the defendant did not base its decision on non-compliance with the rules laid down by those laws, but on the provisions of financial law governing the resolution of financial disputes."*[15]

The reason for not carrying out the examination of the Act LXIII of 1992 in administrative matters was also explained in an abstract way in competition cases, although there was a judgment which did not entirely exclude the interpretation of this Act while assessing the legality of administrative decisions. In a competition law case the appellant stated that the documentation in the administrative proceedings by the competition authority was carried out in breach of the provisions of the Act LXIII of 1992. The administrative court held that *"[a]ccording to Article 1(1) of the Act, its purpose is to guarantee the right of everyone to exercise control over his or her personal data and to have access to data of public interest, except as otherwise provided by a rule of law under this Act. The applicant did not prove in an identifiable manner which natural person was concerned during the defendant's*

[13] Article 16/A (1) (Right to object) The data subject may object to the processing of his data if a) the processing (transfer) of personal data is necessary solely for enforcing a right or legitimate interest of the data controller or data recipient, except if the data processing has been ordered by an Act; b) personal data are used or transferred for the purposes of direct marketing, public opinion polling or scientific research; or c) the exercise of the right to object is otherwise made possible by an Act.

[14] Vas County Court of Hungary 1.K.20.018/2009/33.

[15] Supreme Court of Justice of Hungary Kfv.V.35.180/2009/5.

administrative proceedings or which rules of the processing of personal data were violated. Thus, the court was unable to establish an infringement of data protection law."[16]

In another competition law case, the Supreme Court essentially held that *"[r]egarding the defendant's proceedings, the applicant erroneously referred to the infringement of the Act LXIII of 1992 in the context of the Article 65(4) of the Act LVII of 1996[17]. Data protection rules apply in individual administrative procedures to the extent that the data protection context is regulated by the respective procedural law. In general, on grounds of data protection law, the administrative procedure regulated by law shall not be called into question, as appropriate processing of personal data in these cases is guaranteed by law. From the point of view of data protection, the administrative procedure may be unlawful, including the decision of the authority, if the rules governing the administrative procedure authorize the examination of such aspects. In the absence of this, processing of personal data may be violated in accordance with the procedure set out in the Act LXIII of 199., however, this constitutes an independent data protection procedure, which must be distinguished from the procedure at issue, that is, competition supervision proceedings. The court of first instance rightly pointed out that the legality of the defendant's decision can and shall be assessed in the administrative proceedings on the basis of the Act LVII of 1996, and the administrative action (investigative measure) could not be subject to judicial review under the Act LXIII of 1992*.'[18]

Administrative courts essentially had not dealt with data protection legal issues for about 20 years.

However, this was not due to the fact that the applicants' actions did not attempt to raise issues of data protection law through the reference of the Act LXIII of 1992.

In most of the cases by using this tool they aimed at claiming and proving the unlawfulness of obtaining evidence by administrative authorities, in order to establish errors in the clarification of the facts of the administrative decisions by excluding unlawfully (in breach of data protection rules) obtained evidence.

But we cannot state that the reference to the general data protection act played only such a role. The arguments which sought to demonstrate that public authorities are obliged

[16] Budapest Court of Hungary K.33.024/2004/46.

[17] Article 65(1) -(6) of the Act LVII of 1996 on the Prohibition of Unfair and Restrictive Market Practices (Competition Act) (1) On the summons of the case handler or the competition council proceeding in the case, data recorded in a computing system or on an electronic data storage device (hereinafter collectively: data storage) shall be made available by the possessor of such data storage in a format enabling reading and copying. (2) The case handler and the competition council proceeding in the case shall be entitled to make copies of documents and data stored on a data storage. The case handler shall be entitled to make a forensic copy of the data storage and to inspect its contents using that forensic copy if it is likely to contain data in connection with the conduct under investigation that cannot be retrieved in course of the proper use of the computer. (3) In the process of making an electronic copy of the data stored on the data storage the data shall be recorded in a way that prevents the subsequent manipulation of the data or — if this is not possible due to the type of the data storage — the data shall be recorded using a technology that ensures that it is possible to control the unchanged nature of the data at a later stage. (4) Property may be taken into custody by the case handler by depositing the property into a container suitable for its safeguarding or into a separate room, either of which shall then be locked and sealed. (5) If the property is not available on site, the case handler may take it into custody by obliging the holder of the property to make it available to the Hungarian Competition Authority in an unchanged format, at a specified location and time. (6) Otherwise, custody and seizure shall be subject mutatis mutandis to the provisions of the GRAP Act, with the proviso that with regard to privileged information exemption from confidentiality shall be deemed to have been granted to the holder of the property, with the exception of classified information.

[18] Supreme Court of Justice of Hungary Kfv.37.923/2010/5.

to fulfil their obligations as controllers in the performance of their official functions emerged very quickly and had an impact on their actions. It is apparent, however, that the published case-law lacked a theoretical clarification of data protection law issues and, if it was possible, it emphasized that the lawfulness of an administrative act could be judged solely on the basis of the sectoral administrative rules applicable to it.

2.3. The Evolving Role of Data Protection Authority – Section 25(3)-(4) of the Act LXIII of 1992

According to the original Sections 24-25 of the Act LXIII of 1992 the Data Protection Commissioner a) shall supervise compliance with this Act and other rules of law on data processing b) shall investigate notices lodged with him; c) shall ensure the maintenance of the data protection register.[19]

Under Article 25(1) -(3) of this Act the Data Protection Commissioner shall monitor the conditions of the protection of personal data and of the realisation of public access to data of public interest and data public on grounds of public interest. It shall make proposals for the adoption or amendment of legislation on data processing or on public access to data of public interest and data public on grounds of public interest, and give an opinion on such draft legislation. It may initiate a narrowing or broadening of data categories classified as state or service secrets. Upon observing any unlawful processing of data, the Data Protection Commissioner shall call on the data controller to discontinue the data processing. The data controller shall take the necessary measures without delay and inform in writing the Data Protection Commissioner thereof within 30 days. The Data Protection Commissioner may inform the public of the launching of his investigation, of the fact of the unlawful processing (technical processing) of data, of the person of the data controller (technical data processor) and of the range of processed data.[20]

However, on the 1st January 2004, there was a significant[21] change in the Data Protection Commissioner's supervisory "powers". The legislation gave actual administrative-type supervisory corrective powers to the Commissioner. The Act stated that if the data controller or technical data processor fails to discontinue the unlawful processing (technical processing) of personal data, the Data Protection Commissioner may order in a decision the blocking, deletion or destruction of unlawfully processed data, prohibit the unlawful processing or technical processing of data, and suspend the transfer of data to foreign countries. The decision may not be remedied in administrative way. The data controller, the technical data processor or the data subject may request judicial review from the court against the decision of the Data Protection Commissioner pursuant to paragraph (4) – within 30 days after its receipt – on the grounds of infringement. The Court shall proceed according

[19] Article 24.
[20] Article 25(1) - (3).
[21] See the report of 2005 of the Data Protection Commissioner, 45-46; "*The biggest change in the powers of the Data Protection Commissioner was undoubtedly to order the blocking, erasure or destruction of data processed unlawfully after 1 January 2004, or to prohibit unauthorised processing and to suspend the transfer of data abroad. The controller or processor concerned may turn to a court against the decision of the Commissioner, pending the decision of the court, the data processing shall be suspended and the data shall be blocked. However, the law leaves many important questions unanswered. One of these is what happens if the controller does not terminate the unlawful processing and does not go to court: in addition to 'ordering', the Commissioner does not have any authority to impose a fine or order enforcement*.

to the regulations on lawsuits against public administration of the Civil Procedure Act. Until a final court decision the data concerned may not be deleted or destroyed; the processing of data, however, shall be suspended and the data shall be blocked.[22]

The result of these rules was that the Data Protection Commissioner subsequently participated as defendant to administrative lawsuits brought before the administrative judiciary, in other words, the findings and interpretation of the data protection law set out by the Data Protection Commissioner were subsequently *subject to judicial review*.

The new legislation created new challenges for both the Data Protection Commissioner and the administrative judicial practice. In its changed role, the Commissioner had to draft, edit its "*administrative" decisions*" and conduct its proceedings in accordance with the procedural requirements imposed on administrative decisions and proceedings. Meanwhile administrative law judges had to study the previously unexamined and unexperienced depths of data protection law.

Thus, through the Data Protection Commissioner's decisions, not only the processing of personal data of public bodies could be subject to judicial review, but, as the Commissioner was competent to monitor the processing of all public and private bodies, all controllers and processing operations could, in principle, be subject to the control of the administrative judiciary.

The conditional means, however, that the establishment of the above-mentioned corrective powers of the Commissioner did not result in an "*explosion*" of the number of actions against its decisions. In 2004, a total of 2[23] actions were brought before the administrative court[24].

3. Entry into Force of the Fundamental Law and the Act CXII of 2011 (1st January 2012 – 25th May 2018)

3.1. Introduction of the Ex Officio Data Protection (Supervisory-Type) Administrative Procedure

This period was about the development of the role of the supervisory authority and the extension of the investigative and corrective supervisory powers. It was also another significant step towards a coherent and more detailed data protection administrative judicial practice.

Article VI (2) -(3) of the Fundamental Law on the one hand maintained the Hungarian data protection legal traditions by enshrining the fundamental right to the protection of personal data at the level of the Fundamental Law and on the other hand while triggering a number of procedural and competence consequences it entrusted the monitoring of the exercise of the right to protection of personal data to an '*independent authority*' which was the NAIH.

Section 38(1) established the Authority as an autonomous state administration organ. The Section 38(3) listed the *inter alia* the following tasks of the Authority: the Authority especially a) shall conduct *inquiries* upon notification and ex officio; b) shall conduct

[22] Article 25(4) - (5).
[23] See the Data Protection Commissioner's 2005 report, 35-46.
[24] See the Data Protection Commissioner's 2008 report, 134-135.

administrative proceedings for data protection *ex officio*; c) shall conduct administrative proceedings for the supervision of classified information *ex officio*; d) may bring proceedings before the court in connection with any infringement concerning data of public interest and data accessible on public interest grounds; e) may intervene in actions brought by others. Therefore, the Act CXII of 2011 did not abandon the Authority's so-called "*data protection inquiry*" procedure, an ombudsman-type soft power, but meantime it established the *ex officio* administrative procedure for data protection resulting in legally binding administrative decisions subject to judicial review. The Act on the general rules of administrative procedure shall be applied to the *ex officio* data protection administrative procedure.

The latter was established hand in hand with a toolbox of supervisory investigative and corrective administrative powers, which combine reparative and repressive tasks in order to strengthen the enforcement of privacy rights. At this time data protection administrative procedure could be initiated only *ex officio*.

Section 61(1) defined the legal consequences of the infringement of data protection provisions. According to this in its decision adopted in the data protection administrative proceeding, the Authority may order the erasure, in a manner specified by the Authority, of unlawfully processed personal data or it may impose a temporary or definitive limitation on processing in another way, establish that the personal data have been unlawfully processed, order the rectification of any personal data that are inaccurate, order the blocking, erasure or destruction of unlawfully processed personal data, prohibit the unlawful processing of personal data or prohibit the transfer or disclosure of personal data to foreign countries order the provision of information to the data subject if the controller unlawfully omitted or refused to do so, and impose a fine.

The Act CXII of 2011 could not have stated more clearly that the data subjects had not yet been given a legal opportunity to lodge the administrative procedure with their complaint(s).

The NAIH has become a real "*administrative authority*" with all the consequences.

The administrative justice system found itself also in a completely new position. On the basis of the rules of the Act CXII of 2011 the Hungarian administrative judicial practice began to build its own concept in the field of substantive and procedural data protection law, for instance the competence and the conditions of the application of the investigative and corrective powers of the Authority.

3.2. Questions About the Competence of the Authority

On the basis of the Act CXII of 2011 the Hungarian administrative judicial practice faced almost immediately with specific issues of data protection law and difficulties in resolving them. These questions led to judgments containing basic guidelines to the applications of data protection norms.

In the history of Hungarian data protection law, the first request for a preliminary ruling was submitted by an administrative court in the Weltimmo case[25]. This request concerned the interpretation of Articles 4(1)(a) and 28(1), (3) and (6) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[25] Judgment of 1 October 2015, Weltimmo, C-230/14, EU:C:2015:639.

The request has been made in proceedings between Weltimmo s. r. o., a company which has its registered office in Slovakia, and the Authority concerning a fine imposed by the latter for infringement of Act CXII of 2011 which transposed Directive 95/46 into Hungarian law. Weltimmo run a property dealing website concerning Hungarian properties. For that purpose, it processed the personal data of the advertisers. The advertisements were free of charge for one month but thereafter a fee was payable. Many advertisers sent a request by e-mail for the deletion of both their advertisements and their personal data as from that period. However, Weltimmo did not delete those data and charged the interested parties for the price of its services. As the amounts charged were not paid, Weltimmo forwarded the personal data of the advertisers concerned to debt collection agencies. Those advertisers lodged complaints with the Hungarian data protection authority.

That Authority declared that it was competent, taking the view that the collection of the data concerned constituted processing of data or a technical operation for the processing of data concerning natural persons. Considering that Weltimmo had infringed the Act CXII of 2011, the Authority imposed on that company a fine.

Weltimmo then brought an action before the court which held that the fact that that company did not have a registered office or branch in Hungary was not a valid argument in defence because the processing of data and the supply of data services relating to the Hungarian property concerned had taken place in Hungary. However, that court set aside the decision of the Authority on other grounds, connected with the lack of clarity over some of the facts. Weltimmo appealed on a point of law to the referring court, claiming that there was no need for further clarification of the facts, since, pursuant to Article 4(1)(a) of Directive 95/46, the Hungarian data protection authority in this case was not competent and could not apply Hungarian law in respect of a supplier of services established in another Member State. Weltimmo maintained that, under Article 28(6) of Directive 95/46, that Authority should have asked the Slovak data protection authority to act in its place. The Hungarian data protection authority submitted that Weltimmo had a Hungarian representative in Hungary, namely one of the owners of that company, who represented it in the administrative and judicial proceedings that took place in that Member State. That Authority added that Weltimmo's Internet servers were probably installed in Germany or in Austria, but that the owners of that company lived in Hungary. Lastly, according to that Authority, it followed from Article 28(6) of Directive 95/46 that it was in any event competent to act, regardless of the applicable law.

The Court finally held that Article 4(1)(a) of Directive 95/46/EC must be interpreted as permitting the application of the law on the protection of personal data of a Member State other than the Member State in which the controller with respect to the processing of those data is registered, in so far as that controller exercises, through stable arrangements in the territory of that Member State, a real and effective activity — even a minimal one — in the context of which that processing is carried out. In order to ascertain, in circumstances such as those at issue in the main proceedings, whether that is the case, the court may, in particular, take account of the fact (i) that the activity of the controller in respect of that processing, in the context of which that processing takes place, consists of the running of property dealing websites concerning properties situated in the territory of that Member State and written in that Member State's language and that it is, as a consequence, mainly or entirely directed at that Member State, and (ii) that that controller has a representative in that Member State, who is responsible for recovering the debts resulting from that activity and for representing the controller in the administrative and judicial proceedings relating to

the processing of the data concerned. By contrast, the issue of the nationality of the persons concerned by such data processing is irrelevant.

As for the supervisory powers of the Authority, the Court stated that where the supervisory authority of a Member State, to which complaints have been submitted in accordance with Article 28(4) of Directive 95/46, reaches the conclusion that the law applicable to the processing of the personal data concerned is not the law of that Member State, but the law of another Member State, Article 28(1), (3) and (6) of that directive must be interpreted as meaning that that supervisory authority will be able to exercise the effective powers of intervention conferred on it in accordance with Article 28(3) of that directive only within the territory of its own Member State. Accordingly, it cannot impose penalties on the basis of the law of that Member State on the controller with respect to the processing of those data who is not established in that territory, but should, in accordance with Article 28(6) of that directive, request the supervisory authority within the Member State whose law is applicable to act.

3.3. Scope of the Authority's Corrective Powers

The Authority thus has become an administrative authority not only in its proceedings, but also in terms of administrative sanctions of data protection infringements. As the fundamental nature of these sanctions adversely affect controllers, the conditions and framework under which the Authority may apply them had already been a key issue in administrative lawsuits initiated under the Act CXII of 2011.

The administrative judicial practice based on this Act sought to widen the use of the Authority's toolbox in accordance with the legislative purpose of the Fundamental Law and the Act. Indeed, one of the reasons for the adoption of the Act and the establishment of the Authority was the following: *"[t]he practice of the Commissioner, demonstrated that the powers and tools of the Commissioner did not provide sufficient margin of appreciation and move to investigate and sanction data protection infringements. The spread of information technology, the changing social habits and the new situation created by globalisation require significantly more effective action by public authorities than the system of ombudsman-type Commissioner established in the mid-90s could provide. An administrative authority is a more appropriate organisational form, so it is necessary to establish an authority capable of facing new challenges. The new circumstances necessitate the establishment of a new regulation and organisation in this area that fits into the concept of the Fundamental Law and meets the expectations of the European Union.'*[26]

The Kúria's (Supreme Court of Hungary) approach was in accordance with the this purpose: according to the Kúria "[*t]he Section 61(1)(a) to (g) determines the nature of the measures that may be applied in the decision of the data protection authority. The corrective toolbox covers, for example, the possibility of establishing unlawful processing of personal data, prohibiting the continuation of processing, blocking the unlawfully processed personal data, ordering the termination of their transfer abroad or imposing fines."*[27]

For example, in the context of an *ex officio* prohibition of processing, the reasoning of the court was that " *[p]rocessing of personal data may violate data protection rules in a number of ways with different behaviours and omissions. It is impossible to list them in detail,*

[26] Preparatory document to the Act XCII of 2011.
[27] Kúria Kfv.III.37.911/2017/8.

so the Act CXII of 2011 provides in general for the possibility of prohibiting unlawful processing. Those corrective powers of the Authority must be fulfilled by the defendant in the specific case, having regard to the specific features of the case [...]."[28]

4. The GDPR[29] (2018): Interplay Between the EU and Hungarian Law

4.1. A Revolutionary Change: Data Protection Administrative Procedure at the Request of the Data Subject

On the 25th May 2018, the GDPR entered into force in the above-mentioned circumstances: an increasingly extensive and deepening administrative judicial practice was about to develop. The GDPR did not send the judicial and administrative practice back to the start line.

However, it is worth pointing out some orientations that might determine the interpretation of the GDPR in the future.

Regulation introduced a "*revolutionary*" innovation in the Hungarian law. Article 77(1) of the GDPR provides that, without prejudice to any other administrative or judicial remedy, each data subject shall have *the right to lodge a complaint with a supervisory authority*, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement, if the data subject considers that the processing of personal data relating to him or her infringes this Regulation. In this context, Article 78(1) provides that, without prejudice to any other administrative or non-judicial remedy, every natural or legal person shall have the *right to an effective judicial remedy against a legally binding decision of a supervisory authority* concerning him or her.

The Hungarian legislation – in accordance with Article 41 and 47 of the Charter of Fundamental Rights of the European Union – translated these rules into the Hungarian administrative procedural legislation by opening the possibility of lodging an administrative procedure before the Authority *at the request (complaint) of the data subject*. That is why Section 60(1) of the Act CXII of 2011 provides now that to give effect to the right to personal data protection, the Authority shall bring administrative proceedings for data protection *on the application of the data subject* and may bring administrative proceedings for data protection *ex officio*.

This apparently simple rule has raised a series of questions of interpretation not only in the practice of the Authority but also in the practice of the administrative law courts. Indeed, the general administrative procedure theory makes a clear distinction between administrative procedures initiated at the party's *request* and those initiated *ex officio*. Articles 77 to 78 of the GDPR, apart from requiring a decision by a supervisory authority with legally binding power and effective judicial review, do not contain any further procedural rules governing the specific proceedings under national law, in accordance with the EU law principle of institutional and procedural autonomy of the Member States.

[28] Kúria Kf.VI.37.956/2018/6.

[29] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ 2016 L 119, p. 1) (hereinafter 'the GDPR').

A distinguishing feature of the procedure lodged at the request of the data subject is that in this case the administrative procedure is initiated not on the basis of the professional appreciation of the Authority, but at the will of the data subject. No professional legal help is required in the proceedings before the Authority under the GDPR. However, this leads to the practical consequence that the quality and the content of the requests to carry out the procedure are extremely diverse.

Submitting the application, the data protection administrative procedure is automatically open in accordance with the provisions of the GDPR and national general administrative procedure act. The problem is that while the Authority must draft a sufficiently detailed and justified decision in this type of procedure, as well, the content of the requests often does not allow it to do so, and the Authority often faces incomplete, contradictory and undocumented claims for which even the cooperating controllers find it difficult to provide meaningful answers.

However, this is one of the classic and fundamental questions of the administrative procedure and litigation: the extent to which the administrative authority, in this case the Authority, has an obligation to clarify the facts and to state reasons, and when it reaches the certainty of the decision to establish data protection liability and to impose a serious administrative sanction against an entity as required by the GDPR. It is clearly stated in the case-law that the Authority is not a law-enforcement authority conducting criminal investigation.

The Authority is often confronted with the fact that it can rely only on a small number of evidence, including the data subject's request and the parties' statements made in the course of the procedure, which are evidently contradictory in most cases.

According to the Kúria in principle *"[i]n the proceedings lodged at the request of the data subject, the Authority shall establish the facts to the extent which is necessary for the adoption of the decision and, accordingly, it shall carry out the procedure in order to find the relevant pieces of evidence. However, the Authority is not obliged to seek evidence of the applicant's interest. […]".* It is also established case-law that it is for the applicant to prove the unlawfulness of the Authority's decision in the action before the administrative law court. According to the Curia, it is up to the applicant to prove that the contested decision is vitiated by an infringement of law.

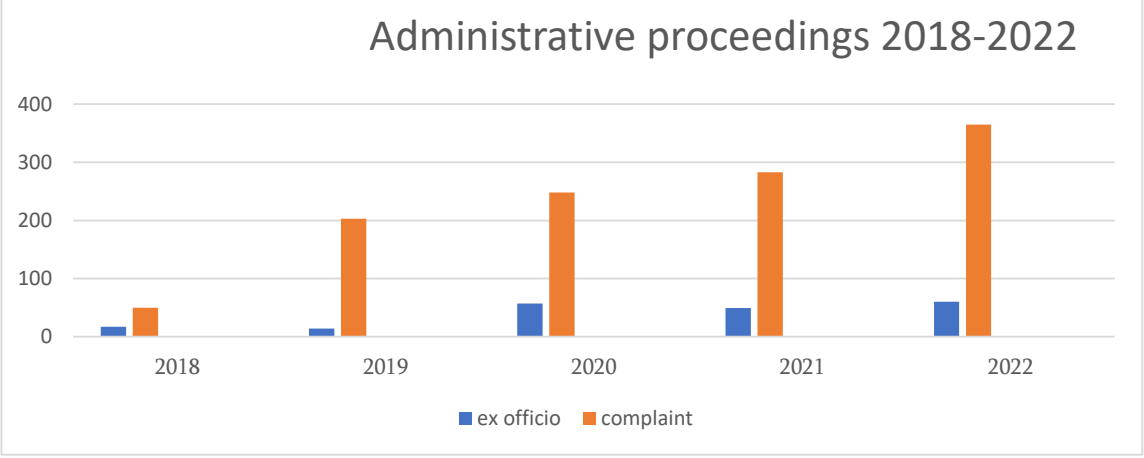
The requests under the GDPR often contain only statements or assumptions, but the data subject is unable to produce any tangible evidence from which any aspect of the specific processing of personal data, the legality or illegality of the latter can be established. It is precisely for this reason that judicial practice has stated, in line with the above, that *"[i]n the absence of processing of personal data actually available, it is not possible to carry out objectively a substantive examination of the request by the Authority."*

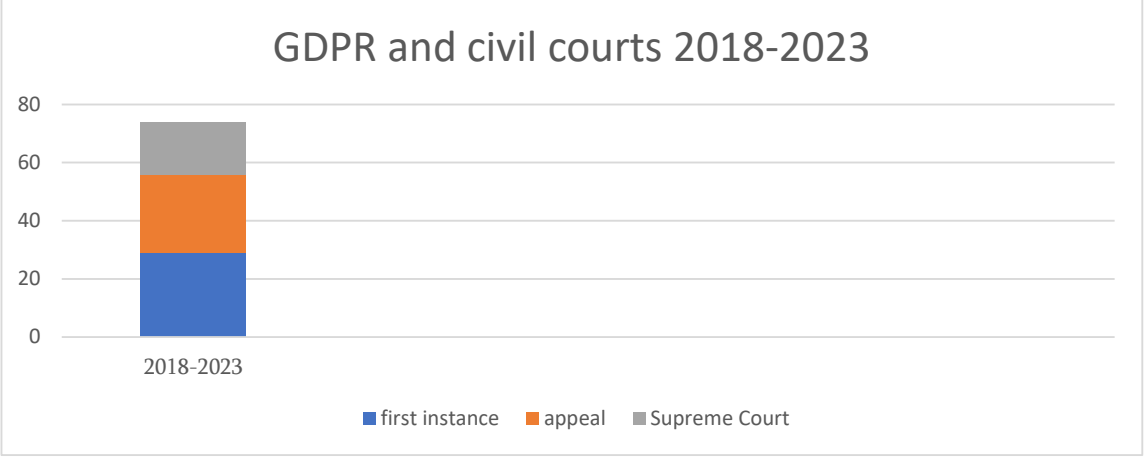
However, before I am going to analyse the most important current issues related to the Authority's corrective powers, let the figures talk about the revolutionary changes introduced in connection with the entry into force of the GDPR. Despite the undoubted procedural difficulties, the GDPR really generated significant changes for data subjects so that they can enforce their data protection rights guaranteed by the GDPR.

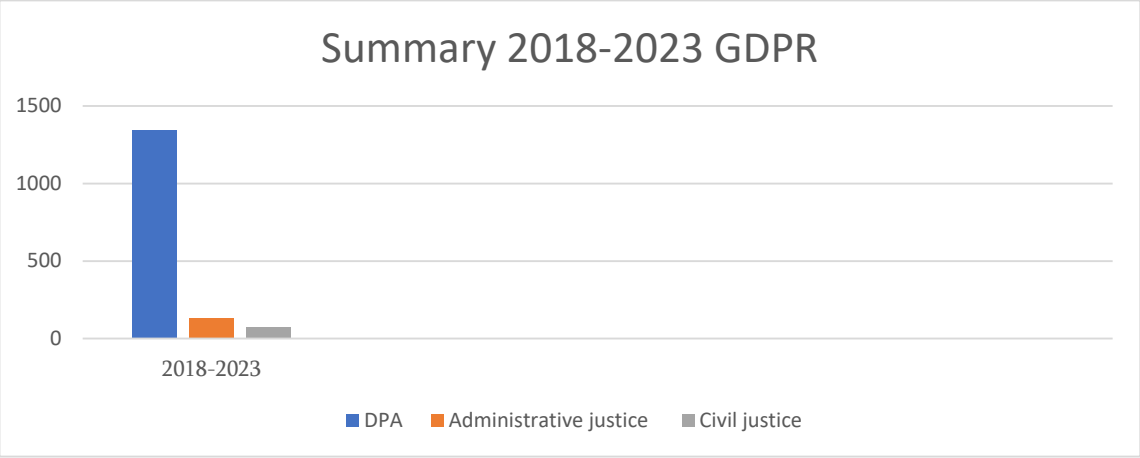
Let us see the statistics before and after the entry into force of the Regulation:

- Number of administrative lawsuits on the basis of former domestic data protection laws 2004-2018 (entry into force of the GDPR): 60;
- Number of administrative lawsuits on the basis of the GDPR 2018-2023: 131 (first instance, appeal and review closed by judgment) [Art. 78 of the GDPR];

- Number of civil lawsuits on the basis of the GDPR 2018-2023: 74 (first instance, appel and review closed by judgment) [Art. 79. of the GDPR];
- Number of references for preliminary rulings 2004-2018 (95/46/EC): 1 (by an administrative court);
- Number of references for prelimimary rulings 2018-2023 (GDPR): 4 (all by administrative courts);
- Number of references for preliminary rulings 2004-2018 (in general): 94;
- Number of references for preliminary rulings 2018-2023 (in general): 27 [15% of the overall Hungarian requests concern data protection issue (!)];
- Number of data protection administrative proceedings *at the request of data subjects* 2004-2018: 0 (as only *ex officio* administrative proceedings were governed by law);
- Number of data protection administrative proceedings *at the request of data subjects* 2018-2023: 1149 [Article 77 (1) of the GDPR];
- Number of data protection *ex officio* administrative proceedings 2018-2023: 197;
- Average percent per year of judicial review on the basis of the overall number of administrative proceedings (*ex officio and complaints*): 9,7%.







4.2. Questions about Corrective Supervisory Powers under the GDPR

Each Member States' supervisory authority is responsible for monitoring the application of the GDPR, in order to protect the fundamental rights and freedoms of natural persons in relation to data processing and to facilitate the free flow of personal data within the European Economic Area. In this regard, Article 57(1)(a) GDPR provides that each supervisory authority shall on its territory enforce the application of the GDPR.

This duty applies regardless of whether the supervisory authority acts *ex officio* or on the basis of a complaint.

However, in order to carry out this task the supervisory authorities must have effective toolsets, which allow them to take action against infringements of Regulation. For this reason, Article 58(2) GDPR provides for a set of corrective powers that a supervisory authority can use.

According to Article 58(2) of the GDPR each supervisory authority shall have all of the following corrective powers:

> (a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;
>
> (b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;
>
> (c) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;
>
> (d) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;
>
> (e) to order the controller to communicate a personal data breach to the data subject;
>
> (f) to impose a temporary or definitive limitation including a ban on processing;
>
> (g) to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19;

(h) to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met;

(i) to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case;

(j) to order the suspension of data flows to a recipient in a third country or to an international organisation.

"Strong enforcement", "consistent and homogenous application of the rules", "equivalent powers for monitoring and ensuring compliance", *"equivalent sanctions for infringements"* and *"same tasks and effective powers, including (…) corrective powers"* are all called for by the recitals of the GDPR.[30] According the EDPB the consistent application of the corrective powers of the supervisory authorities is of key importance for the consistent level of protection in the European Economic Area.[31] This view is in accordance with that of data protection theory: *"[t]he GDPR this strengthens the system of the supervisory authorities and their independence and powers within a dedicated Chapter VI, and creates a mechanism for cooperation and consistency in Chapter VII."*[32]

However, the interpretation of the interplay of these supervisory powers raised questions especially with regard to the possible collision of the *ex officio* corrective powers of the Authority and the rights of the data subjects. This question was referred to the European Court of Justice to preliminary ruling by a Hungarian administrative court which can fundamentally determine the strength and the scope of the corrective powers of the data protection supervisory authorities in the future.

By its questions, the referring court asks, in essence, whether Article 58(2), in particular subparagraphs (c), (d) and (g), of the GDPR must be interpreted as meaning that the national supervisory authority, in exercise of its corrective powers, may order the data controller or processor to erase unlawfully processed personal data even in the absence of an express request by the data subject under Article 17(1) of the GDPR? In the event that the answer to the first question is that the supervisory authority may order the data controller or processor to erase unlawfully processed personal data even in the absence of a request by the data subject, is that so irrespective of whether or not the personal data were obtained from the data subject?

As regards the part of the decision ordering the erasure of personal data in the specific case, the applicant submits that Article 58(2)(d) of the GDPR does not give the Authority power to issue such an order. The applicant argues that the obligation on the data controller

[30] Recital 7, 10, 11 and 129 GDPR. See also Opinion 39/2021 on whether Article 58(2)(g) GDPR could serve as a legal basis for a supervisory authority to order ex officio the erasure of personal data, in a situation where such request was not submitted by the data subject (Adopted on 14 December 2021) See <edpb.europa.eu/system/files/2022-01/edpb_opinion_202139_article_582g_gdpr_en.pdf>.

[31] Opinion 39/2021 on whether Article 58(2)(g) GDPR could serve as a legal basis for a supervisory authority to order ex officio the erasure of personal data, in a situation where such request was not submitted by the data subject (Adopted on 14 December 2021) See <edpb.europa.eu/system/files/2022-01/edpb_opinion_202139_article_582g_gdpr_en.pdf>.

[32] Christopher KUNER-Lee A. BYGRAVE-Christopher DOCKSEY: The EU General Data Protection Regulation (GDPR) – A Commentary. Oxford University Press, Oxford, 2020. 942-943.

to erase data irrespective of whether the data subject has so requested flows from Article 5 of the GDPR rather than from Article 17(1) of that regulation, because the erasure under Article 17 of the GDPR can only be interpreted as a right of the data subject and the second part of the sentence in Article 17(1) can only be interpreted in the context of the exercise of that right, not independently but subject to the exercise of that right by the person concerned.

Before this request for preliminary ruling by decision No 3110 of 23 March 2022 the Hungarian Constitutional Court stated that, under Articles E (2) and (3) and VI (4) of the Hungarian Fundamental Law and in accordance with the GDPR — as EU legislation guaranteeing the uniform application of data protection and the freedom of information — the Authority has power to order *ex officio* the erasure of unlawfully processed personal data, including where there is no request by the data subject.

It seems that the Hungarian administrative court of first instance does not share fully the positions of the Constitutional Court. In this court's view, the right to erasure under Article 17 of the GDPR clearly must be interpreted as a right of the data subject and Article 17(1) does not establish two separate legal grounds for erasure. Instead, the second part of the sentence in that paragraph ('the controller shall have the obligation to erase [the data subject's] personal data without undue delay') is a subsequent obligation on the data controller deriving from the first part of that sentence. In consequence, contrary to the Board's Opinion 39/2021, this court is of the view that the right of erasure under Article 17 of the GDPR may only be interpreted as a right of the data subject. This is supported by the fact that the original text of the GDPR in English refers to the data controller's obligation using the conjunction 'and' between the first and second parts of the sentence in Article 17(1).

According to the court the question to be determined is, therefore, whether, irrespective of any exercise of his or her right by the data subject, the national supervisory authority may oblige the data controller or processor to erase the unlawfully processed personal data and, if it may, on what legal basis; in answering that question, it must be borne in mind, in particular, that Article 58(2)(c) of the GDPR is expressly predicated on a request to exercise the rights of the data subject and that Article 58(2)(d) provides in general terms that processing operations must be in compliance with the GDPR, while Article 58(2)(g) refers directly to Article 17 which, as explained above, likewise cannot be interpreted regardless of the need for an express request by the data subject to erase personal data.

For the Board to assess whether the power of the supervisory authorities under Article 58 (2)(g) of the GDPR applies even in the absence of a request for erasure from the data subject, it first had to consider whether Article 17 of the GDPR imposes an obligation on the controller only following a request from the data subject, or if this obligation is independent thereof. In this regard the Board found that Article 17 of the GDPR provides for two separate cases for erasure that are independent from each other: I. the erasure at the request of the data subject, and II. the erasure as a standalone obligation of the controller. This conclusion of the Board is supported by the fact that some cases set forth in Article 17(1) of the GDPR clearly refer to scenarios that the controllers must detect on their own as part of their obligation for compliance with the provisions GDPR, and by the rationale to allow supervisory authorities to ensure the enforcement of the principles enshrined in the GDPR even in cases where the data subjects are not informed or aware of the processing, or in cases where not all concerned data subjects have submitted a request for erasure. Based on the above reasoning, the EDPB concludes that Article 58(2)(g) of the GDPR is a valid legal basis for a

supervisory authority to order *ex officio* the erasure of unlawfully processed personal data in a situation where such request was not submitted by the data subject.[33]

The question can also be raised as to whether the data subject has the right to the illegality or whether the will (self-determination) of the data subject can set aside the whole GDPR even if the Authority found the processing totally unlawful. The judgment is expected in 2024.

4.3. Temporary Corrective Powers and the Online World

One of the biggest challenges is monitoring the online world and effectively intervening when necessary in "*data protection no-go zones*", especially on the dark web and several social media platforms. The Hungarian legislator - acting on the authority given by the GDPR[34] - therefore has given new powers to the Hungarian supervisory authority by modifying the Act CXII of 2011 and establishing the so-called "*blocking corrective powers"*: the order to remove and the order to render inaccessible electronic personal data.

As a first step and as a provisional measure to prevent the unlawful processing of personal data, the Authority may require also the hosting service provider or the intermediary service provider providing also hosting services on certain issues of electronic commerce services and information society services that processes the data published through an electronic communications network to temporarily remove the electronic data the publication of which serves as grounds for an authority proceeding for data protection or administrative audit by the Authority if in the absence thereof, the delay would cause an unavertable and severe violation of the right to personal data protection and

a) the data subject of the published data is a child, or

b) the published data is sensitive data or criminal personal data.

A procedural decision on the temporary removal of electronic data shall be communicated to the party subject to the removal obligation without delay. The party subject to the removal obligation shall be obliged to temporarily remove the electronic data within one working day from the communication of the procedural decision on the provisional measure by the Authority.[35]

Secondly as a provisional measure to prevent the unlawful processing of personal data, the Authority may order that the electronic data the publication of which serves as grounds for an authority proceeding for data protection or administrative audit by the Authority be rendered temporarily inaccessible. The electronic data may be rendered temporarily inaccessible where in the absence thereof, the delay would cause an unavertable and severe

[33] Opinion 39/2021 on whether Article 58(2)(g) GDPR could serve as a legal basis for a supervisory authority to order ex officio the erasure of personal data, in a situation where such request was not submitted by the data subject Adopted on 14 December 2021.

[34] Article 58(6) of the GDPR 6. Each Member State may provide by law that its supervisory authority shall have additional powers to those referred to in paragraphs 1, 2 and 3. The exercise of those powers shall not impair the effective operation of Chapter VII. See also*: "Article 58 is directly applicable. Hence, DPA's can rely on it directly when exercising their powers. However, Article 58 also leaves room for national legislation, both with regard to questions of procedural law and those of additional tasks."* KUNER- BYGRAVE-DOCKSEY (2020) 944.

[35] Section 61/A (1) -(2).

violation of the right to personal data protection, and any other measures, including temporary removal by the Authority under section 61/A (1) remained ineffective, and

a) the data subject of the published data is a child, or

b) the published data is sensitive data or criminal personal data.

The Authority shall communicate a procedural decision ordering the electronic data to be rendered temporarily inaccessible by public notice. The public notice shall be posted on the bulletin board and published on the website of the Authority for five days. The day of the communication of the procedural decision shall be the third day following the posting of the public notice. An obligation imposed by the procedural decision of the Authority shall apply to all electronic communications service providers without the need for an explicit provision to that effect.[36] The Authority may impose a procedural fine ranging from one hundred thousand forints (260 EUR) to twenty million forints (50.000 EUR) on an electronic communications service provider that fails to comply with its obligation set out in this section.[37]

4.4. Conflicts between the Authority and the Civil Courts

By introducing the administrative proceedings at the request of the data subject, it is not uncommon at all that data subjects lodge a complaint before the Authority and simultaneously an action before a civil court often with the same content, based on the same data protection provisions, asking the Authority (and thus the administrative court in case of judicial review) and the civil courts to interpret the same GDPR norm in the same case.

In this case Articles 77 to 79 of the GDPR almost necessarily give rise to a conflict between the administrative and judicial paths. The Court of Justice has interpreted Articles 77 and 79 of the GDPR from the point of view of the definition of the competences established in those provisions. The aforementioned articles confer on individuals rights enforceable in parallel, but the parallel exercise of those rights may give rise to uncertainty in relation to legal certainty, as is the case in the dispute of the case C-132/21. Since, in accordance with national procedural legislation, decisions of the Authority are not binding on the civil courts, it is not inconceivable that a civil court may adopt a decision contrary to that of the supervisory authority in relation to the same facts.

The role of an administrative court pursuant to the powers conferred by Article 78 of the GDPR is to review the decisions of the supervisory authority. The competences of the supervisory authority also define the competences of the administrative court, given that the latter may carry out an examination of lawfulness in respect of points of law falling within the scope of the supervisory authority's sphere of competence. The administrative court has an obligation to review the findings contained in the supervisory authority's decision on the infringement of the GDPR, the civil courts, acting pursuant to the powers provided for in Article 79 of that regulation, can give a final judgment on the same point of law. The judgment of the civil court lacks the authority of *res iudicata* in the dispute in the main proceedings because the parties to the proceedings are not identical. It can occur that the administrative court has to examine the same facts and the commission of the same infringement — and interpret the same EU and national legislation — as those/that in respect of which the civil court has already given final judgment. In accordance with national procedural law, even though the judgment of the civil court is not binding on the administrative court, [the latter

[36] Section 61/B (1) -(4).

[37] Section 61/B (6).

court] cannot disregard the general principle of legal certainty, whereby court decisions are binding on everyone (Article 6 of the Law on the organisation of the courts).

The parallel between competences at the vertical level is also problematic, given that the objective set out in recital 117 of the GDPR — according to which the establishment of supervisory authorities in Member States, empowered to perform their tasks and exercise their powers with complete independence, is an essential component of the protection of natural persons with regard to the processing of their personal data —, the achievement of which is an obligation incumbent on the Member States under Article 51(1), would be partially restricted if the legal action preceded the administrative appeal. In so far as it is permitted to bring the administrative appeal and the legal action in parallel, any final court order made first would be binding on the supervisory authority at the time of adjudicating on a complaint lodged on account of the same facts. In that situation, therefore, the competences of the supervisory authority as provided for in Article 58 of the GDPR would be restricted.

In case C-132/21 the Court finally ruled that Article 77(1), Article 78(1) and Article 79(1) of the GDPR read in the light of Article 47 of the Charter of Fundamental Rights of the European Union, must be interpreted as permitting the remedies provided for in Article 77(1) and Article 78(1) of that regulation, on the one hand, and Article 9(1) thereof, on the other, to be exercised concurrently with and independently of each other. It is for the Member States, in accordance with the principle of procedural autonomy, to lay down detailed rules as regards the relationship between those remedies in order to ensure the effective protection of the rights guaranteed by that regulation and the consistent and homogeneous application of its provisions, as well as the right to an effective remedy before a court or tribunal as referred to in Article 47 of the Charter of Fundamental Rights.

Since the Hungarian legislation does not contain any regulations regarding parallel legal remedies, the issue is not closed yet. The Authority respects the judgments of the civil courts even if, as this was the case in C-132/21, the legal position of the civil judge is contrary to the Authority's interpretation. The referring court was right though by stating that this situation resulting from the GDPR, may lead to the infringement of one of the most important EU principle: the rule of law. Numbers show in Hungary that the number of civil remedies is negligible compared to the administrative ones. No wonder, since the Authority has much stronger powers, its administrative proceeding is free from red tape, on the other hand civil court procedures are claimed to be excessive and rigid and the compensations for (reputation) damages are relatively low.

5. Conclusions

GDPR has proved to be a game changer. It has brought revolutionary changes, the fundamental and complete transformation of the role of supervisory authorities, its proceedings and relationship with the judiciary. GDPR has radically raised privacy-awareness across organisations of any kind and it is a radical breakthrough in data subjects', data controllers' and the courts' (!) beliefs and behaviours with regard to the importance of data protection.

Over the past 30 years, Hungarian data protection law has come a long way, with a number of substantive, procedural and organisational changes. Nevertheless, the tendencies are clearly moving in one direction: due to the brutal growth of the digital age and the data-based economy and services, the exercise of the right to the protection of personal data

requires strong and effective powers. The development of data protection law in Hungary has already directed the organisational and procedural legal framework to an administrative-type model by establishing a more and more effective toolbox of corrective powers before the GDPR and in some sense even before the Act CXII of 2011.

As regards the role of administrative justice in this process, the initial passive, rather abstaining attitude has been overturned by the above process, and the Hungarian administrative judiciary increasingly and more and more actively claims a decisive role in interpretation of data protection law.

However, this process is far from over, on the contrary we are at the very beginning. The case- law of the Court is still evolving and important questions of substantive and procedural law remain to be answered.

Paraphrasing József Attila's famous lines, based on historical experience there'll be always enough reason to look up the file which violates someone's rights. The real question is whether data protection legislation remains a dead letter or by means of legally and practically enforceable supervisory powers, the principles and rules protecting our privacy come to life.

Bibliography:

1. Act LVII of 1996 on the Prohibition of Unfair and Restrictive Market Practices (Competition Act).
2. Data Protection Commissioner's 2008 Report, 134-135.
3. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) OJ 2016 L 119, p. 1 / GDPR.
4. The Fundamental Law of Hungary (25 April 2011).
5. *Kuner C., Bygrave L.A., Docksey C.,* The EU General Data Protection Regulation (GDPR) – a Commentary, Oxford University Press, Oxford, 2020, 942-943.
6. Opinion 39/2021 on whether Article 58(2.g), Adopted on 14 December 2021.
7. Kúria Kf.VI.37.956/2018/6.
8. Kúria Kfv.III.37.911/2017/8.
9. Budapest Court of Hungary K.33.024/2004/46.
10. Judgment of 1 October 2015, Weltimmo, C-230/14, EU:C:2015:639
11. Report of 2005 of the Data Protection Commissioner, 45-46;
12. Supreme Court of Justice of Hungary Kfv.37.923/2010/5.
13. Supreme Court of Justice of Hungary Kfv.V.35.180/2009/5.
14. Vas County Court of Hungary 1.K.20.018/2009/33.

Zviad Gabisonia*

Legal Challenges of Personal Data Protection During the Processing of Big Data

In the rapidly evolving landscape of modern technologies, the scale of Big Data processing is on the rise, presenting a challenge to the legal protection of personal data. Big data processing serves as the "fuel" for modern technologies, including artificial intelligence.

"Big data" is a well-established term in information technology science, and its official definition is nearly nonexistent. According to the most widely recognized definition, this term refers to a large dataset, whose collection, management, and processing significantly surpasses the capacities of traditional databases and their corresponding programs.

The article explores the legal protection of personal data in the processing of big data, using the legal frameworks of two of the most technologically advanced countries, the USA and China, as examples. The article illustrates the positive and negative factors associated with the expansion of big data processing concerning personal data protection.

Keywords: *Big Data, Data protection, Personal data, The US Clean Network Initiative, Global Initiative on Data Security.*

1. Introduction

In the fourth industrial revolution, where cutting-edge technologies such as artificial intelligence rely on machine learning, deep learning, and neural network analytical models, the foremost challenge is the protection of personal data. Any cutting-edge technology that utilizes the internet network involves extensive information processing. This gives rise to a significant challenge concerning the legal aspects of personal data protection.

On June 14, 2023, the Parliament of Georgia passed a new law, "On Personal Data Protection." The first article of this law explicitly states its primary objective: "to protect basic human rights and freedoms, including the rights to personal and family life, personal space, and communication inviolability when processing personal data".

* Professor at Business and Technology University, Head of the doctoral program "Digital Governance and Artificial Intelligence in the Public Sector", USAID expert in artificial intelligence law.

The new edition of the law directly reflects the EU regulations[1] in addressing challenges related to personal data. The law is applicable to the processing of data by automatic and semi-automatic means within the territory of Georgia, as well as the processing of data by non-automatic means that are part of the file system or processed for input into the file system. Additionally, it covers the processing of data using technical means available in Georgia by a data controller registered outside Georgia, unless those technical means are solely used for data transit.[2]

The processing of personal data is directly connected to the concept of "Big Data" processing, which serves as the primary "fuel" for all modern technologies. "Big data" is a well-established term in information technology science, and its official definition is nearly nonexistent. According to the most widely recognized definition, this term refers to a large datasets, whose collection, management, and processing significantly surpasses the capacities of typical, traditional databases and their corresponding programs.[3]

The purpose of the article is to study and analyze the essence of Big Data and the legal challenges associated with the processing of personal data within its framework.

2. The Essence of Big Data

Napoleon was known to assert, "90% of war is information." Presently, technological and business organizations are actively pursuing a novel natural resource. This resource holds greater value than oil and is more crucial than capital. This resource can be acquired, but it cannot be owned. It exists in every country, yet obtaining it proves to be challenging. The world's leading companies recognize that without it, they face inevitable failure, yet outdated management methods often hinder its acquisition. This new natural resource is known as Big Data.

The public goods of the information age are easily visible — smartphones in pockets, laptops in bags, and information technology systems in offices. However, what is less noticeable is the information itself. Over the last twenty years, the accumulation of data has reached a point beyond which people's imagination and perception of reality are entering a new phase. The quantitative change in information has led to a qualitative transformation. Scientific fields such as astronomy and geophysics have introduced the term Big Data, a concept now pervasive across all spheres of human activity today.

There is no singular, perfect definition of big data. The initial concept revolved around the idea that the volume of information to be analyzed had expanded to a scale where traditional storage methods like USB or other data carriers were no longer practical. As a result, computer engineers needed new data carriers that could facilitate the analysis of extensive volumes of information. This is how completely new programs for processing big data appeared, such as, for example, Google's MapReduce and its open-source equivalent, Yahoo's Hadoop. These programs facilitated the utilization of a network of multiple computers to address diverse tasks.

[1] <https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en> [07.01.2024].
[2] The Law of Georgia "On Personal Data Protection", 3144-XIms-Xmp, 14/06/2023, Art. 2 (1).
[3] *Franks B.,* Taming the Big Data Tidal Wave: Finding Opportunities in Huge Data Streams with Advanced Analytics, New Jersey: John Wiley & Sons, Inc., 2012.

The ability of internet companies to collect substantial data about individuals and legal entities provided them with the motivation to invest in and develop technologies and programs capable of analyzing this information, making it more valuable for business.

However, this is just the beginning. The era of big data will challenge global norms, questioning how we live and interact with the world. It will challenge centuries-old traditions, practices, and fundamental human understanding, including how decisions are made and how we perceive the world.

Entering the era of big data marks, the beginning of radical changes. To comprehend the magnitude of the information revolution, this is demonstrated by the current trends across almost all sectors of society. Our digital world is constantly expanding. For example, Google.com collects more than 50petabytes of information per day, which is more information than all the world's libraries combined. Facebook.com uploads tens of millions of photos per hour, while Youtube.com uploads up to two billion videos per month. Information is accumulated in the fields of finance, banking, healthcare, insurance, agriculture, transport and logistics.

Big data is essentially "raw" information. Similar to raw natural resources, such as crude oil, it must undergo a process of "refinement," grouping, and shaping before it can be utilized as a usable product. This constitutes a massive data structure that enables artificial intelligence to analyze an increasing amount of information through self-development, ultimately delivering precise analytics in various fields with more comprehensive calculations. Big data carries an immense volume of resources, making its analysis unattainable through traditional methods of information analysis. Big data can be used to generate and analyze observations that would be otherwise unattainable with small-scale analysis methods. Consider a voice message, a tweet, an email, personal photos, and videos on social networks, or even your transactions on world-renowned websites like amazon.com, ebay.com, Alibaba.com, Taobao.com, or local platforms like Georgian vendoo.ge or liloshop.ge, passport scans, photos of hamburger or sandwich, or even electrocardiogram recordings. All these elements have the potential to form the foundation of big data.

Big data is acknowledged as a contemporary technology for processing, analyzing, and distributing substantial volumes (arrays) of both structured (interrelated) and unstructured (e.g., text messages, images, videos, audio) digital information. It encompasses 8 dimensions or 8Vs: Volume - the size of data; Value – the importance or worth; Veracity – reliability and accuracy; Visualization – processing and external presentation; Variety – diversity; Velocity – speed; Viscosity – data retention in memory; and Virality – mass spreading.[4]

The evolution of new internet technologies will open up additional opportunities for harnessing big data. For instance, the advancement of the 5th generation of mobile internet - 5G, will not only enable the concept of “smart things”, but also ensure “smart cities” are consistently online, facilitating the extraction and processing of immensely large amounts of data. Artificial intelligence will gain the capability to acquire precise information about individuals, encompassing their preferences in terms of desires, food, technology, housing, love for nature, and even political views. According to some scientists, this development is seen as a precursor to significant dangers. For example, the globally renowned modern historian Yuval Noah Harari emphasizes that artificial intelligence, without proper legal regulation, poses a substantial threat to humanity, and its danger does not necessarily lie in physically harming individuals. The primary issue is that, through the analysis of big data,

[4] *Jolia G.,* Education and Employment in the Digital Environment, Tbilisi, 2021, 36 (in Georgian).

artificial intelligence will have the capacity to observe human emotions and not only understand individuals' interests and attitudes toward various subjects and events, but it will also have the ability to analyze and understand even the innermost emotions that a person may not be aware of themselves. An illustrative example of this is a case where artificial intelligence, through a woman's internet browsing habits, inadvertently focused on sites reflecting behaviors related to small children. Consequently, the program analyzed the woman's emotions and inferred that she was pregnant. Just a few days later, during a visit to the doctor, the woman discovered that she was indeed expecting a child. The perils of artificial intelligence and the necessity for regulation will be discussed separately below, we won't stop the discussion here.

In the course of the fourth industrial revolution, data has become a more valuable resource than land or oil were during the first and second revolutions. When this resource, much like "crude oil," undergoes processing and becomes suitable for use, it will present an incredible opportunity for technological companies and humanity as a whole.

Big data is integral to the multi-stage and multi-layered technological war between the world's two largest economies: the US and China.

3. The US “Clean Network” Initiative

The trade and technology war between the United States of America and China has undergone numerous rounds. However, the primary cause of the conflict between them revolves around the question of who can better control the most valuable resource of the modern era – big data. The ban on popular mobile applications like TikTok and WeChat by the United States is one of the manifestations of the ongoing battle over big data.

The so-called "Clean Network" initiative, published by the US State Department, involves a public statement by the United States aimed at protecting American citizens and encouraging other countries to join this initiative. In the preamble of the "Clean Network" initiative, the statement of the US Secretary of State is cited, urging "all freedom-loving countries and companies to join The Clean Network".[5]

The "Clean Network" initiative includes "Clean Carrier", "Clean Store", "Clean Apps", "Clean Cloud", "Clean Cable", "Clean Path".

The “Clean Carrier” initiative entails the US policy aimed at ensuring that online information carriers from the People's Republic of China are not connected to US communications networks. Such companies pose a threat to US national security and should not be involved in US international telecommunications services.

The “Clean Store” initiative aims to remove untrusted apps from US mobile app stores. Specifically, apps created by Chinese companies pose threats to US privacy, propagate viruses, engage in content censorship, and disseminate disinformation. The official statement asserts that the most sensitive personal and business information on Americans' mobile phones must be safeguarded and protected from theft and exploitation by any third party.

The “Clean Apps” initiative signifies that pre-installations and downloads on Chinese-made smartphones should undergo inspection to determine whether these applications utilize technologies from Huawei or other Chinese companies that might pose a threat to the personal rights and freedoms of citizens in the United States or other countries.

[5] “We call on all freedom-loving nations and companies to join the Clean Network”, <https://2017-2021.state.gov/the-clean-network/> [07.01.2024].

The "Clean Cloud" initiative signifies that the most sensitive personal information of US citizens and the most valuable intellectual property of American businesses, including details about COVID-19 vaccine research, will be processed and stored exclusively on cloud systems, avoiding the use of programs, hardware, applications, and smartphones provided by Chinese companies with anti-American affiliations such as Alibaba, Baidu, China Mobile, China Telecom, and Tencent.

The "Clean Cable" initiative, as asserted by the US State Department, ensures to safeguard the security of undersea cables connecting America to the global Internet, mitigating the risk of subversion by Chinese intelligence systems at a hyper-scale. They are also ready to work with foreign partners to ensure that undersea cables around the world are protected and America will be uncompromising in this regard.

On April 9, 2020, US Secretary of State Pompeo unveiled the “Clean Path” initiative. This initiative entails the US State Department mandating a "Clean Path" for 5G internet traffic entering and exiting US diplomatic facilities.

The US points to the fact that Chinese 5G internet traffic development companies Huawei and ZTE operate under the directives of the Chinese Communist Party, leading to a lack of trust from the US. This move is aimed at safeguarding American citizens and businesses from unauthorized intrusions by Chinese companies through 5G internet traffic.

The significance of Georgia signing a memorandum with the US on "Security of 5G networks,"[6] on January 14, 2021, is noteworthy, through this action, Georgia practically joined the "Clean Network" initiative.

The document highlightes the importance of safeguarding communications networks from interference or manipulation. The memorandum emphasizes the necessity to support reliable and trustworthy network hardware and software vendors in 5G markets, considering national security risk profile assessments and, also, the need to promote infrastructure that effectively protects 5G networks from unauthorized access or interference. According to the document, when evaluating suppliers in the market, it is crucial to be guided by criteria such as the rule of law, security environment, ethical supplier practices, and compliance with safety standards and industry best practices.

According to the memorandum, the parties recognize that 5G suppliers must provide products and services that facilitate innovation and enhance efficiency. These products and services should ensure fair competition and foster further development in the market with the involvement of maximum participants.

By signing the memorandum, Georgia became the 53rd member country of the "Clean Network" initiative of the US State Department. As evident from official statements of the US State Department, member countries (numbering over 50) and their more than 180 telecommunication companies, controlling more than 2/3 of the world's gross domestic product, have publicly affirmed their commitment to the principles of the "Clean Network" initiative.[7] This commitment will encourage the use of hardware and software products from trusted suppliers to secure the Internet network infrastructure, safeguard the privacy of citizens, prevent unauthorized access to telecommunications infrastructure, and ensure national security.

The "Clean Network" initiative of the US State Department is primarily aimed at the People's Republic of China and its high-tech companies, it should be regarded as one of the

[6] <http://www.economy.ge/index.php?page=news&nw=1617> [07.01.2024].
[7] <https://2017-2021.state.gov/the-clean-network/> [07.01.2024].

manifestations of the "technological war" between America and China.[8] The US State Department explicitly asserts that Chinese high-tech companies utilize their equipment to manipulate the personal information of citizens from different countries for their own purposes and there is a significant risk that this information could be transferred to the Chinese government to address various security issues. This poses a threat not only to the disclosure of personal information of citizens but is also directed against the national interests of countries.

In addition to the principles defined above, the “Clean Network” initiative explicitly states that it protects the most sensitive information of US citizens and its companies from aggressive and harmful actions by external actors. For example, such as the Chinese government. The main goal of this initiative is to protect US digital assets, mainly big data, from falling into the hands of Chinese competitors, even through legal means (for example, based on information officially obtained from "Tik Tok"). As mentioned above, big data serves as a kind of fuel for the development of technologies such as artificial intelligence, and dominance in the field of artificial intelligence will practically provide a significant advantage to the competitor. Eric Schmidt, the former CEO of Google, expressed concern about this in a public speech. He stated, "By 2020, we will be overtaken by the Chinese; by 2025, they will surpass us, and by 2030, they will dominate the field of artificial intelligence." Therefore, he urged the US government to take swift and effective steps in developing a state strategy for artificial intelligence and the protection of big data.

There is indeed reason for concern. According to numerous studies, Chinese companies already possess approximately ten times more information in the field of big data compared to the US. Each day, Chinese companies Alibaba and Tencent (the company that owns the WeChat app) update, process, and utilize the personal information of up to 1 billion people. China's leaders often state that the country's economic and military development hinges on the advancement of technologies in virtually every field of applied science, this includes robotics, genetics, space technology, drones, pharmaceuticals, microprocessor and microchip technologies, as well as modern solar energy technologies.

4. “Global Initiative on Data Security” of the People's Republic of China

China, as one of the world leaders in artificial intelligence science, has devoted all its scientific resources to perfecting big data analytics in the past few years. However, at the same time, it is compelled to overcome the restrictions imposed by its competitors recently. An example of this is the "Clean Network" initiative of the US State Department mentioned above, which is primarily directed against China. Beijing appeared to back down and responded with a " Global Initiative on Data Security."

On September 8, 2020, China's Ministry of Foreign Affairs published the " Global Initiative on Data Security " on its official website.

The initiative notes that "the phenomenal development of the information technology revolution and the digital economy is transforming the way of production and life, exerting a broad impact on the social and economic development of states, the global governance system, and human civilization. The rapid growth of data and its integration as a key element of digital technology has played a crucial role in promoting innovative development and shaping people's lives, It has implications for the security of states and economic and social

[8] Ibid.

development, therefore, we call on all states to equally prioritize development and security, adopting a balanced approach to technological progress, economic development, and the protection of national security and public interest. States should promote an open, fair, and non-discriminatory business environment for mutual benefit, profit, and common development. At the same time, states have the responsibility and the right to protect important data and personal information related to their national security, public safety, economic security and social stability."

The initiative emphasizes that China welcomes the participation of governments, international organizations, information technology companies, non-governmental organizations, individuals, and all other actors to encourage joint efforts to ensure data security based on broad consultation, shared contributions, and mutual benefits. All parties should strengthen dialogue and cooperation on the basis of mutual respect and support each other to build a society with a shared future in cyberspace of peace, security, openness, cooperation and order.[9]

To ensure this, China proposed to the states:

- To be able to protect data security with a comprehensive, objective and evidence-based method and to maintain an open, secure and stable supply chain of products and services in the field of information and communications technology (hereinafter referred to as - "ICT").
- Oppose ICT activities that disrupt or steal important data from the critical infrastructure of other states or use the data to conduct activities that undermine other States' national security and public interests.
- Take measures to prevent activities that endanger personal information through the use of ICTs and to oppose mass surveillance against other states and the unauthorized collection of personal information of other states with ICTs as a tool.
- To encourage companies to abide by the laws and regulations of the State where they operate. States should not request domestic companies to store data generated and obtained overseas in their own territory.
- Respect the sovereignty, jurisdiction and governance of data of other States, and shall not obtain data located in other States through companies or individuals without other States' permission.
- Should States need to obtain overseas data out of law enforcement requirement such as combating crimes, they should do it through judicial assistance or other relevant multilateral and bilateral agreements. Any bilateral data access agreement between two States should not infringe upon the judicial sovereignty and data security of a third State.
- Providers of ICT products and services must refrain from installing security programs (commonly known as "backdoors") in their products and services to guard against the illegal acquisition of users' data for the purpose of control or manipulation of users' systems and devices.
- ICT companies should not seek illegitimate interests by taking advantage of users' dependence on their products, nor force users to upgrade their systems and devices. Products providers should make a commitment to notifying their cooperation partners and users of serious vulnerabilities in their products in a timely fashion and offering remedies.[10]

[9] <https://www.flyingnets.com/en/> [07.01.2024].
[10] Ibid.

- China calls on all states to support this initiative and confirm the above commitments through bilateral, regional and international agreements. They also welcome global ICT companies to support this initiative.
- In the "Global Initiative on Data Security" of September 8, 2020, China presented initiatives that countered the arguments made by the US State Department to China and its major technology companies.

5. Big Data Achievements and Challenges

"Big data" elicits mixed evaluations among scientists and other segments of society. Undoubtedly, there are both positive and negative aspects to consider.

Modern medical knowledge and the ability to make accurate diagnoses rely on a small number of talented and qualified individuals. Clearly, the majority of people do not possess comprehensive knowledge of the advancements achieved in this field across various countries. This limitation could stem from the constraints of human memory or the limited time available to keep pace with the latest developments in this domain. Certainly, a significant portion of medical information and scientific knowledge is accessible through open or closed scientific databases on the Internet or on the websites of information agencies. However, this information is scattered, making it challenging to access systematized knowledge that is easily comprehensible. Access to top-tier medical diagnosis still remains dependent on geographic location and financial resources.

Next-generation artificial intelligence technologies will change all that. Beyond the numerous social implications associated with doctor visits, diagnosis relies on the collection of vast amounts of data including symptoms, anamnesis, medical history, environmental factors, and the prediction of potential outcomes such as diseases. Finding correlations and making predictions is what deep learning (so-called Deep Learning) methods are being developed for. With a sufficient amount of data, such as accurate medical records, the utilization of artificial intelligence in diagnosis transforms any medical specialist into a superdiagnostic. They will become a doctor equipped with the experience of diagnosing and treating tens of millions of patients, possessing the ability to detect hidden correlations and possessing a perfect memory. This is what the Chinese artificial intelligence medical company “RX Thinking”, which operates on the “smart medicine” model, aims to develop. The company was established by a Chinese artificial intelligence researcher with extensive experience from Silicon Valley in the United States. This startup specializes in instructing and refining Chinese AI algorithms to develop super precise diagnostic programs. Following the diagnosis, the results can be swiftly transmitted to any region across China.[11] It's interesting that rather than aiming to replace doctors with algorithms, the intention is for it to serve as an assistant application for doctors during the diagnostic process. This means aiding doctors in formulating the right strategy for diagnosis. Additionally, it doesn't compel doctors to entirely depend on its data and recommendations. However, considering that the algorithm continues to evolve by assimilating information from each new medical case, it progressively reduces diagnostic errors. Simultaneously, it may prompt for additional information to finalize the diagnosis process.[12] Once sufficient information is uploaded to convince the algorithm, the

[11] <https://medicalfuturist.com/top-artificial-intelligence-companies-in-healthcare/> [07.01.2024].
[12]<https://healthitanalytics.com/news/top-12-artificial-intelligence-innovations-disrupting-healthcare-by-2020> [07.01.2024].

program can accurately predict a potential disease or provide an accurate diagnosis by analyzing the symptoms. Moreover, during symptom analysis, it displays a percentage on the monitor indicating the likelihood of identifying the exact disease based on those symptoms.

The application does not disregard the doctor, who always has the option to make a diagnosis different from the recommendations of the application. However, the application is built on a foundation of over 400 million diagnoses and continuously learns, analyzes, and scans new information or medical publications to provide updated knowledge and trends.[13]

Hence, doctors in the future will be tasked with focusing entirely on comforting patients and exploring positive human factors, which remain essential even today.

Demonstrating positive trends in the development of artificial intelligence through big data extends beyond the field of medicine alone. Numerous examples abound in agriculture, (such as the diagnosis of soil analysis via drones and their assistance in the advancement of agricultural technologies, which promises tremendous results for significantly enhancing yields. Monitoring and sending data through drones of state-sponsored projects for AI program analysis, etc.), transport and logistics, military and defense, etc. in the fields.

When using big data technology, it is imperative to respect fundamental human rights and freedoms, along with principles of information security and dissemination, as there exists a fundamental risk of their unequal utilization. The security of big data, like to a state's territorial borders, holds paramount strategic significance. It serves as a nourishing and decision-making tool for the intelligent software environment.[14]

Despite the benefits and positive impacts of big data, the era of big data also gives reasons for concern. As big data becomes increasingly proficient at predicting various aspects of the world and our place within it, we may find ourselves unprepared for its potential effects on our daily lives and personal freedoms. People's perception of the world and institutions was formed in those eras and realities where the scarcity of information was the basis of our development. And now we are moving into an era in which it becomes completely possible to obtain and process all kinds of information, which will allow the relevant organizations to manipulate people in an unimaginable way. For example, Facebook's business strategy is to create a user-friendly platform where 2.5 billion people can freely share personal photos and videos about themselves, their family, and friends. As of today, this network collects a vast amount of personal information about people, which allows the platform to analyze the behavior of each person, understand exactly what emotions they have, what they like, what they don't like, how they dress or eat, and offer them exactly the ads encouraging them to make purchases. This allows the platform to place premium prices on ads for companies that are targeting their micro-segment of customers.

Facebook founder and CEO Mark Zuckerberg stated during a US Senate hearing, "Because we understand what you're interested in, we can show you specific ads tailored to you." This statement elucidates how Facebook learns and analyzes the behaviors, preferences, daily routines, emotions (via likes and other "emojis"), as well as political, religious, and even sexual attitudes of its 2.5 billion users daily, while scrolling through your Facebook feed you encounter customized advertisements tailored specifically for you.

In 2019, commissioned by Netflix Films, Karim Amer and Jehane Noujaim's documentary "The Great Hack" delves into the influence of the social network "Facebook" on the shaping of advertising and political views. This journalistic investigation is particularly significant in

[13]<https://www.technologyreview.com/2020/07/15/1004743/a-new-rx-ai-for-operations-in-health-care/> [07.01.2024].

[14] *Jolia G.,* Education and Employment in the Digital Environment, Tbilisi, 2021, 37 (in Georgian).

relation to Donald Trump's victory in the 2016 US presidential elections and Great Britain's exit from the European Union (Brexit). The film highlights the connection between these two significant political events and it relates to the activities of the renowned British big data analytics company (Cambridge Analytica) and its direct involvement in both of these campaigns. In particular, "Cambridge Analytica" employees later gave testimony confirming how they used the personal information of US and UK citizens on social networks, mainly Facebook, and manipulated the will of still "neutral" voters, which led to the victory of Trump in the USA, and the victory of "Brexit" supporters in the UK referendum. During a US Senate hearing, Mark Zuckerberg acknowledged the misuse of users' personal information on his platform and issued an apology, he also stated that he was unaware of his company's employees' involvement in Project Alamo.[15]

In 2020, the documentary film "The Social Dilemma" by director Jeff Orlowski premiered on the Netflix platform. Based on interviews with psychologists, IT specialists, programmers, and professionals in the internet field, the film effectively portrays how social networks and search engines can manipulate people using artificial intelligence and big data. Manipulation is not limited to converting network "users" into good "consumers" to encourage them to purchase as many products as possible (even if they often do not need these products), but it also includes changes in people's behaviors, preferences, and political or different views, which undoubtedly violates human rights and freedoms.

6. Conclusion

In the modern world, processing big data presents a significant challenge to safeguarding personal data. In the article, we aimed to present both the positive and negative aspects of big data processing from a legal perspective. Indeed, the evolution of big data is an irreversible process, and technologies based on artificial intelligence will continue to advance methods for processing large datasets over time. In this process, personal data protection issues will face big challenges, which require constant transformation of relevant legislation and adaptation to new challenges. Accordingly, I think it is important to modify the functions of the Personal Data Protection Service in Georgia[16] in such a way that it can respond to the ever-increasing personal data processing challenges with fast and flexible mechanisms.

Bibliography:

1. Law of Georgia "On Personal Data Protection", 3144-XIms-Xmp, 14/06/2023.
2. *Jolia G.*, Education and employment in the digital environment, Tbilisi, 2021, 36-37 (in Georgian).

[15] Project Alamo, the leading project of Donald Trump's 2016 presidential campaign, in which, according to journalists reportedly involved employees from Cambridge Analytica and Facebook. Utilizing big data and artificial intelligence, they allegedly targeted and influenced swing voters, which contributed to Trump's victory in the election. See, <https://www.thealamo.org/alamo-plan/preservation/black-paper/index.html>; <https://semantiko.com/project-alamo/> [07.01.2024].

[16] <https://personaldata.ge/ka> [07.01.2024].

3. *Franks B.,* Taming the Big Data Tidal Wave: Finding Opportunities in Huge Data Streams with Advanced Analytics, New Jersey: John Wiley & Sons, Inc., 2012.
4. <https://healthitanalytics.com/news/top-12-artificial-intelligence-innovations-disrupting-healthcare-by-2020> [07.01.2024].
5. <https://www.technologyreview.com/2020/07/15/1004743/a-new-rx-ai-for-operations-in-health-care/> [07.01.2024].
6. <https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en> [07.01.2024].
7. <https://medicalfuturist.com/top-artificial-intelligence-companies-in-healthcare/> [07.01.2024].
8. <https://www.thealamo.org/alamo-plan/preservation/black-paper/index.html> [07.01.2024].
9. <http://www.economy.ge/index.php?page=news&nw=1617> [07.01.2024].
10. <https://2017-2021.state.gov/the-clean-network/> [07.01.2024].
11. <https://semantiko.com/project-alamo/> [07.01.2024].
12. <https://www.flyingnets.com/en/> [07.01.2024].

Iva Katić [*]

Data Protection Officer as Preventive Mechanism of Infringements with Regard to the Tasks Prescribed by the General Data Protection Regulation

The demands made by the data protection officer, for most of the work collective, is additional burden, which makes work of data protection officer extremely lonesome. The essence of this position is to pay attention within the organization that there is no infringement of the Data Protection Law, which makes this position extremely responsible. Precisely in regard to above mentioned it may be said that the data protection officers may, by reason of the nature of their tasks, act preventively on the entire organization in relation to an infringement, and consequently on respect for one of the fundamental human rights, especially right to personal data protection.

Keywords: *Data protection officer, Personal data protection, Prevention of infringements.*

1. Introduction

Personal data is all around as. Even if an information at glance doesn't seem to be qualified as personal data, companies should think twice.

Name, date of birth, home address, e-mail address, IP address, ID number, health data such as dioptric of an individual, fingerprint, car registration number, photo and many other data are personal data.

In accordance with European law, Article 8. Under the EU Charter of Fundamental Rights, the protection of personal data is recognized as a separate fundamental human right.

Until the entry into force of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation; hereinafter GDPR), the main EU legal instrument on the protection of personal data was the Personal Data Protection Directive[1].

However, due to the expansion of modern technologies, there was a need to reform legislation so that the legal framework could relatively effectively monitor personal data processing in the modern and digital age.

In this regard, the GDPR entered into force as a technologically neutral regulation that has become a pioneer in the protection of personal data on a global scale and a well-known role model.

[*] Secretary of the Cabinet Office at Croatian Data Protection Authority.

[1] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

More than five years ago, GDPR has sparked a lot of public interest and has forced many subjects to make an X-ray in their organizations.

To comply with the data protection law controller must have the ability to carry out all the tasks prescribed by the law.

In recent years, it has become evident how valuable a data protection officer is for the organization.

It is highly recommended to appoint data protection officer within organization. The data protection officer can have a strong preventive effect on the organization in which they operate.

Appointment of the proper data protection officer may reduce the possibility of a personal data breach and infringements.

2. Preventive Impact of the Data Protection Officer Role within Organization

Let's imagine a complaint by the data subject complaining that the company has posted the personal data of data subject on the company's website.

Published data contained data subject's vehicle identification number (chassis number), general data about the motor vehicle and data on the damage under specific number.

At first glance, the average individual would say that published data was not personal data. However, by entering the chassis number on several websites person may receive feedback on the vehicle such as engine marking, color code or date of production and more.

In the beginning person cannot know too much about the owner of the motor vehicle, but having a chassis number enables to find out even exact identity of the vehicle owner.

Let's imagine that company didn't appoint data protection officer and claims that chassis number is not a personal data.

How will this company comply with transparency obligation set out in the Data Protection Law?

In this regard, within the company someone should have had identified the chassis number as personal data and should have had determined the legal basis for the processing and met transparency obligation by including information about legal basis for processing in the privacy notice.

According to the GDPR, data subject is an identified or identifiable natural person, directly or indirectly. Identifiers such as certain factors related to the physical, physiological, genetic, mental, economic, cultural or social identity of an individual contribute to identification[2].

Identity of the driver of the vehicle can be subsequently established by additional information, indirectly, by one or more factors specific to the specific person, location data, etc., therefore the chassis number of the vehicle should be considered as personal data.

Data protection officer (if appointed or had been adequately appointed) would have recognized the link to identity behind the "chassis number" and would have been familiar with the definition of the personal data. After identification of the personal data, the data protection officer would identify the legal basis for the processing prior to publication on the

[2] Regulation (EU) 2016/679 of the European parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/ec (General Data Protection Regulation), Article 4. Paragraph 1.

website, and then, in accordance with the principle of data minimization[3], would advise to publish the personal data only if it were necessary and inform the data subjects about such processing.

Data protection officer is an employee or external expert who has the high professional ethics and knowledge about Data Protection Law.

Such a person, must be aware of the obligations imposed by the Data Protection Law, must continuously monitor decisions taken by the supervisory authorities within the European Economic Area as well as the judgments of the Court of Justice of the European Union, recommendations and opinions of the supervisory authorities, as well as the European Data Protection Board guidelines.

Data Protection Officer is a type of inspection within an organization. For this reason, it is very important to have internal knowledge of the structure of the organization. Processes carried out by organizations, as well as the means of processing must be familiar to data protection officer.

An individual who is considered as an inspection within an organization should be of a certain type of personality. Not every person, however skilled, can communicate successfully with authority. Indeed, data protection officer has to oppose ideas that are in conflict with Data Protection Law. Also, not every person can address criticism to their colleagues and demand that the provisions of the regulations on the protection of personal data be complied with.

A major problem in practice is appointment of an inadequate person. When appointment is purely formal, organization cannot benefit.

2.1. Advisory Task Impact on the Prevention of Infringements

The data protection officer should have an advisory role. Whenever a new procedure or technology is to be introduced in an organization, data protection officer must be involved in the project in order to be able to act preventively on mechanisms that would risk personal data breaches or infringements.

Early involvement in the project is crucial. When developing new technologies into processes, a good expert will take into account data protection by design and default[4] and thus integrate some of the safely measures such as possibility of deleting the data after the retention period(s) has ended, ensure that access to personal data is restricted only to certain personnel who need to perform a specific task with personal data and only to a specific set of personal data they need to know, to ensure that the data cannot be read, copied, modified or removed without authorization (e.g. need-to-know basis), ensure that access to data can only be possible after authorized personnel have been successfully identified and authenticated etc.

GDPR is a risk-based regulation. The DPO should constantly assess the risks in order to be able to identify processing within the organization which may be problematic from the data protection aspect. For example, if a company's personal data is systematically and extensively profiled or new technological solutions are used in the processing of personal data, such as the application of the "Internet of Things", or personal data are being processed

[3]Ibid, Article 5. Paragraph 1.
[4] Ibid, Article 25. Paragraph 1.

by linking, comparing or checking matches from multiple sources, the data protection officer must light a red flag.

Data protection officers are not a burden for the company. They are not designated to forbid personal data processing. They serve to ensure that the processing of personal data is GDPR compliant. Data protection officer is here to look for a solution that will meet the demands of the employer as well as the requirements of the GDPR. DPO is a kind of a mediator.

However, if company doesn't see that it will be beneficial for them to seek an advice from the data protection officer and include them in project which include data processing it should bear in mind it could be investigated for not doing so.

Belgian DPA[5] investigated regional government agency for tourism which resulted in reprimands for not proactively including data protection officer in processing task prescribed by the Law which consequently led to a breach of Article 38 (1) GDPR and Article 39 (1) GDPR.

2.2. Monitoring Compliance with the Provisions of the Laws as Mechanism for Prevention of Infringements

The data protection officer is authorized to conduct audits. They can be initiated either on the basis of an external signal, for example, an individual submits a complaint to the company and data protection officer investigates the circumstances of the complaint or may be an internal signal based on a complaint or notice from a trade union commissioner, labor council, whistle-blower, but also any employee.

Company must provide the data protection officer with all the resources and relevant access to carry out the audits. Also, the company should inform its employees of the data protection officer's authority to conduct investigations (it would be good to give explicit guidance through the company's internal rules). A similar notice should also be made known to external service providers, suppliers, members of the supervisory board and all others who come into contact with personal data in the company.

Regular auditing can certainly detect (in time) certain problems in the processing of personal data and prevent a personal data breach.

2.3. Awareness-raising and Training of Staff Involved in Processing Operations

Most of the personal data breaches stem from an error by an employee of the controller, of course error can happen, however, it can also be prevented by proper education of employees.

Company in Norway[6] mistakenly conducted a credit check on one of the owners of another company which resulted in fine of 200,000 NOK. Infringement was caused by lack of familiarity with the system they used for requesting credit reports.

Case happened in Cyprus[7] where a typing mistake occurred with passport number in during the process of updating client's data in Hellenic Bank. After a while other individual

[5] APD/GBA (Belgium) - 162/2022 - GDPRhub [30.09.2023].
[6] Datatilsynet (Norway) - 20/04401 - GDPRhub [30.09.2023].
[7] Commissioner - 12.10.001.011.001 - GDPRhub [30.09.2023].

verified information, and his new passport had the number that the bank employee had mistakenly typed as previous client's passport number, hence other client has partial access through the web banking platform to other person's personal and financial data. This case didn't result with imposing a fine but it was demanded that the controller take some appropriate measures.

The Information Commission Office[8] reprimanded Ministry of Justice for confidentiality breach. Several people had access to confidential waste documents after they were left in prison holding area.

The Polish DPA[9] fined district court with 6,387 euros because an employee lost three USB sticks contain draft ruling and personal data of an unidentified number of individuals.

In this regard it is important to emphasis that one of the obligations arising from the General Data Protection Regulation[10] is to take appropriate organizational protection measures, which, among other things, include raising awareness within the organization.

Such an obligation of the controller is linked to the tasks of the personal data protection officer, whose task is to raise awareness among employees and train staff in order to prevent data breach.

There are numerous of examples in practice where the data protection officer would have a preventive effect on a personal data infringement only if awareness-raising activities on the importance of personal data protection were carried out within the organization.

When it comes to employee error, the intention to breach personal data is infrequent. As a rule, employees are not aware of the risks arising and their mistakes. They are also unaware of this incident, which they have to report in order to have a rightful influence on the impact that the infringement will have on the data subject.

2.4. Providing Advice in the Data Protection Impact Assessment Process

According to the GDPR[11] where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

Such an obligation of the controller is linked to the tasks of the personal data protection officer; whose task is to provide advice requested as regards the data protection impact assessment.

A data protection impact assessment serves to identify a high risk to the rights and freedoms of individuals when processing personal data.

[8] ICO (UK) - Ministry of Justice (1) - GDPRhub [30.09.2023].

[9] UODO (Poland) - DKN.5131.12.2020 - GDPRhub [30.09.2023].

[10] Regulation (EU) 2016/679 of the European parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Article 32. Paragraph 1.

[11] Regulation (EU) 2016/679 of the European parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/ec (General Data Protection Regulation), Article 35. Paragraph 1.

Some of the factors/examples[12] that may involve high risk are: a financial institution that verifies its clients through the Anti-Money Laundering (AML) or fraud database, a biotechnology company offering genetic tests directly to consumers to assess and predict risks for the development of diseases/health risks, a company that produces behavioral or marketing profiles based on the use or navigation of their websites, General Hospital that keeps patient records, a private investigator who keeps details of criminal convictions or offences, extensive collection of genealogical information about the families of persons belonging to a particular to a religious group, the processing of data generated by the use of the so-called "Internet of Things" applications if the use of data has (or may have) a significant impact on the daily life and privacy of individuals.

The risk under assessment relates not only to the risks related to the right to the protection of personal data, but also to other rights and fundamental freedoms such as the right to private and family life, the right to freedom of expression and information, etc.

Therefore, for example, if a company wants to track the location of an employee's vehicle, there is a risk of processing personal data on the location of an employee at a time other than official opening hours, as it may affect their private and family life.

When a high risk is identified, it is necessary to assess whether it can be mitigated by applying appropriate technical and organizational protection measures. If the risk cannot be reduced, it is advisable to waive the processing of personal data.

In this process, the personal data protection officer plays a key role, depending on the advice, a personal data breach or infringement may be successfully (or unsuccessfully) prevented.

In the case of high risks which cannot be reduced by technical and organizational measures to 'eligible risk', the obligation referred to in Article 36 of the GDPR shall follow, which is a prior consultation of the supervisory authority.

2.5. Cooperation with the Supervisory Authority

The data protection officer shall cooperate with the supervisory authority. Cooperation may be initiated on its own initiative or at the initiative of the supervisory authority.

The data protection officer's relationship with the supervisory authority may affect compliance with personal data protection regulations.

3. Conclusion

The appointment of a data protection officer within an organization may act as a preventive mechanism for infringements of data protection rules, which sources from the nature of its tasks. Among other tasks, data protection officer must advise controllers and employees who are carrying out data processing, must encourage a culture of respecting the right to personal data protection within organization and must monitor the compliance with data protection regulations. Their appointment, enabling the performance of their tasks in a timely manner, taking into account their advices may ensure that personal data law is not violated. The link between data protection officer and preventive mechanism with regard to infringements of the law are related their risk-based actions in general which (provided that

[12] <https://azop.hr/wp-content/uploads/2023/09/DPO-prirucnik.pdf>, (173-178).

the data protection officer is an adequate person) is always two steps in ahead thinking how to improve compliance with the law and how to mitigate risks and balance business activities with request to protect personal data protection right.

Bibliography:

1. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
2. Regulation (EU) 2016/679 of the European parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
3. <https://gdprhub.eu/index.php?title=APD/GBA_(Belgium)_-_162/2022> [30.09.2023].
4. <https://gdprhub.eu/index.php?title=Datatilsynet_(Norway)_-_20/04401> [30.09.2023].
5. <https://gdprhub.eu/index.php?title=Commissioner_(Cyprus)_-_12.10.001.011.001> [30.09.2023].
6. <https://gdprhub.eu/index.php?title=ICO_(UK)_-_Ministry_of_Justice_(1)> [30.09.2023].
7. <https://gdprhub.eu/index.php?title=UODO_(Poland)_-_DKN.5131.12.2020> [30.09.2023].
8. <https://azop.hr/wp-content/uploads/2023/09/DPO-prirucnik.pdf> [30.09.2023].

Saba Elizbarashvili*

Processing of Personal Data Through the Use of Drones (Review of International Standards and Compliance with Georgian Legislation)

Video recording represents one of the most pervasive forms of data processing. The advancement of modern technologies, including drone aerial photography systems, has introduced a host of new challenges concerning the protection of personal data. The accessibility and user-friendliness of drones enable individuals to process personal data of a considerable number of subjects, thereby significantly increasing the risk of violating the provisions outlined in Georgia's existing and forthcoming laws "on Personal Data Protection". The paper examines the standards established for the legality of drone data processing and offers relevant recommendations to data controllers.

Keywords: *Personal data protection, Personal data processing, Modern technologies, Video recording, Drone.*

1. Introduction

With the rapid advancement of technology, which includes drones, and the integration of smart systems, the potential for data collection reaches an almost boundless scale. GPS technology, frequently a built-in feature of drones, enables the tracking and recording of the drone's location as well as that of any surveillance targets.[1] In addition, the drone can be equipped with a sound recording device, as well as simple, night vision, and/or thermal imaging (thermographic) cameras that can detect the location of a person based on body heat. The drone can also be equipped with 3D scanners, as well as WiFi and/or Bluetooth devices, and recognition systems for mobile devices,[2] which provide the ability to track a person's location via their mobile phone. The use of such systems by drones can have a significant negative impact on an individual's data protection and privacy rights.

Advanced surveillance technologies can integrate a drone's high-quality audiovisual recording and storage capabilities with data analytics tools like facial recognition software, gait analysis, and other biometric assessment systems, which enables targeted surveillance of individuals.[3] Furthermore, the size and maneuverability of drones afford the capability to observe, track, and follow targets from a considerable distance without the monitored

* Master of law at Ivane Javakhishvili Tbilisi State University; Lawyer of the Legal Department at Personal Data Protection Service of Georgia.

[1] *Tarr T., Tarr J. A., Thompson M., Wilkinson D.,* Data Protection, Privacy and Drones, Clyde & Co LLP, 2022, 1.

[2] Spanish Data Protection Agency, Drones and Data Protection, 2019, 1, <https://www.aepd.es/es/documento/guia-drones-en.pdf> [04.09.2023].

[3] *Tarr T., Tarr J. A., Thompson M., Wilkinson D.,* Data Protection, Privacy and Drones, Clyde & Co LLP, 2022, 1.

individual being aware of such surveillance.[4] Therefore, a key challenge with drone use is the limited awareness of the data subject which, on the one hand, is manifested in the lack of information about data processing itself and on the other hand in the identity of the data controller (drone operator).[5]

Personal data is defined as "any information relating to an identified or identifiable natural person",[6] drone operators that record or/and process images, video, voice, biometric data, geolocation, or telecommunications data related to an identified or identifiable individual should be considered as data controllers, (except in cases where the drone is used solely for household or personal purposes).[7] Therefore, in cases where drones are used under the conditions mentioned above, drone operators, as data controllers, are subject to both the General Data Protection Regulation (GDPR) and the rules established by the Georgian Law on Personal Data Protection.

It should be noted that, taking into account the European practice, excluding national or international legislation on personal data protection, various types of specialized documents may address issues related to personal data protection in the context of drone usage. These documents may include manuals prepared by supervisory bodies, internal regulations governing civil aviation, and documents developed by the European Union in this field. This article discusses the main data protection standards and recommendations in the process of using drones, including the structure, content and goals of individual documents regulating the issue.

2. Drone Operator/Data Controller Obligations

Regarding the issue of personal data protection in the process of drone use, we find essentially similar approaches across Europe. In particular, special attention is focused on the obligations of the drone operator and the need to ensure proper data protection guarantees. Among these, notable obligations include transparency, informing the data subject, ensuring data security, and practicing data minimization. Furthermore, it is essential to consider data protection standards, such as Data Protection by Design and by Default, and to prepare an impact assessment on data protection when developing a new product or service.

2.1. Transparency and Obligation to Inform the Data Subject

Article 15 of the Law of Georgia "On Personal Data Protection" outlines the obligatory procedure for disclosing information to the data subject. This requirement holds particular relevance in drone-related data processing scenarios, as in most cases, the data subject remains unaware of their data being processed and the identity of the data controller.

[4] Ibid.

[5] Information Commissioner's Office (ICO), UK, Additional Considerations for Technologies other than CCTV, October 2022, 36.

[6] The Law of Georgia on "Personal Data Protection", 5669-rs, 28/12/2011, art. 2, sub-para. "a".

[7] In the case of using a drone solely for family, economic, or personal purposes, the direct operation of the drone by an individual may be exempt from obligations established by personal data protection legislation. However, if the data obtained as a result of such operation is subsequently processed (such as distributing photo, video, or audio material on social networks), the requirements set forth by legislation will apply as standard.

In many instances, due to the large number of data subjects, it becomes challenging, if not impossible, to individually inform all subjects within the drone's filming area (e.g., in a stadium, on the street, etc.). Accordingly, drone operators are tasked with finding "innovative" methods to provide information to individuals whose personal data is processed as a result of drone use. In cases where it is particularly challenging or requires a disproportionately large effort, the data controller should endeavor to inform the subjects through alternative means, which can be expressed, for example: officially registering the drone with the civil aviation authority, displaying appropriate signage in the area of drone operation, publishing a privacy notice on the data controller's website, or presenting privacy notice through alternative channels.[8]

It is crucial for the data subject to easily discern the identity of the drone operator or data controller.[9] Therefore, to facilitate the identification of the responsible party controlling the drone, it is advisable for both the drone and its operator to remain within the field of vision of the data subject.[10] To enhance visibility, the drone operator may choose to wear easily identifiable attire. Additionally, it is advisable for the operator to be prepared to furnish requested information to interested individuals via a QR code. This QR code can direct the data subject to a website link containing details about the personal data protection policy.[11] Furthermore, to ensure adherence to the principle of transparency, the drone should be equipped with an appropriate signaling system, such as a flashing light or audible sound, to alert the data subject to the ongoing recording by the drone.[12]

In each specific case, it is essential to assess the most effective method of informing the data subject, whether it involves placing information signs or cards in the vicinity of the drone's operation, publishing information on social media or in print media, distributing informational brochures, displaying posters, or other suitable means.[13] The main aim is to ensure that the data subject is informed about the data processing activities, including details about the data controller, the purpose of processing, and the rights of the data subject.

2.2. Data Minimisation Principle

According to Article 4 "G" of the Law of Georgia "On Personal Data Protection", data may only be processed to the extent necessary to achieve the relevant legal purpose. Additionally, the data must be adequate and proportionate to the purpose for which they are processed.

[8] Information Commissioner's Office (ICO), UK, Additional Considerations for Technologies other than CCTV, October 2022, 36.

[9] The UK Civil Aviation Authority, The Drone and Model Aircraft Code - For Flying Drones, Model Aeroplanes, Model Gliders, Model Helicopters, and other Unmanned Aircraft Systems Outdoors in the Open A1 and A3 Categories, Protecting people's privacy (Points 20 to 25). Published: October 2019, Last updated: January 2023. Point 22, 32, <https://register-drones.caa.co.uk/drone-code/the_drone_code.pdf> [04.09.2023].

[10] The GDPR (General Data Protection Regulation) and Drones, 2018, <https://aerialworx.co.uk/gdpr-and-drones/> [04.09.2023].

[11] The Data Protection Commission (DPC) of Ireland, Guidance on the Use of Drones, 2022, 4, <https://www.dataprotection.ie/en/dpc-guidance/guidance-on-the-use-of-drones> [04.09.2023].

[12] Ibid, 5.

[13] Spanish Data Protection Agency, Drones and Data Protection, 2019, 4, <https://www.aepd.es/es/documento/guia-drones-en.pdf> [04.09.2023].

The principle of data minimization is particularly crucial in the process of data processing using a drone. On one hand, in some cases, the number of subjects involved in such data processing can be particularly large, which can exacerbate the threat to the rights of the data subjects. However, on the other hand, various technical facilities make it relatively easy to achieve the minimization of drone data.

Minimizing interference with human privacy and data protection rights can be achieved by planning and considering the following issues/actions in advance: 1. specific flight route, 2. appropriate type of drone and its equipment, 3. management of collected data.[14]

The data collection and storage systems integrated into the drone can be configured by default to prevent the collection and processing of unnecessary amounts or types of data. This can be achieved, (for example, by automatically depersonalizing the data, such as blurring the images of individuals moving in the area captured by the camera),[15] to avoid indiscriminate or excessive data processing, the drone operator must adhere to the principles of data minimization, as well as consider options for anonymization and pseudonymization.[16]

To adhere to the principle of data minimization, the data collection systems installed on drones should feature on-off functionality as needed, and the captured visual angle of the frame should be limited to the specific purpose of data processing (for example, if the drone is being used to inspect a particular section of a damaged roof, there is no need for a 360-degree angle of view).[17]

To minimize data, it is advisable for the drone operator to limit the number of people and identifiable objects (eg, a license plate) in the frame as much as possible. This goal can be achieved by conducting flights during times of the day when the lowest concentration of people is observed in a specific area. Additionally, it's preferable to conduct video/audio recording or photography only at specific moments when necessary, rather than throughout the entire flight.[18]

To prevent such invasive photo or video recording, which grossly violates people's privacy, the drone operator must be aware of the technical capabilities of the drone being used. In particular, the operator should be aware of how well the drone records images, the extent to which it can zoom in on a shot (known as "zoom"), and whether it is technically possible to start and stop filming during flight.[19] To gain a better understanding of this information and become acquainted with the drone's capabilities, it is advisable for the operator to conduct test flights in a controlled environment before flying in public spaces.[20]

---

[14] *Tarr T., Tarr J. A., Thompson M., Wilkinson D.,* Data Protection, Privacy and Drones, Clyde & Co LLP, 2022, 3.

[15] The Data Protection Commission (DPC) of Ireland, Guidance on the Use of Drones, 2022, 4-5. <https://www.dataprotection.ie/en/dpc-guidance/guidance-on-the-use-of-drones> [04.09.2023].

[16] Personal Data Protection Service, Worldwide Practice, June/2022, 11-12. <https://personaldata.ge/ka> [04.09.2023].

[17] The Data Protection Commission (DPC) of Ireland, Guidance on the Use of Drones, 2022, 5, <https://www.dataprotection.ie/en/dpc-guidance/guidance-on-the-use-of-drones> [04.09.2023].

[18] Spanish Data Protection Agency, Drones and Data Protection, 2019, 3, <https://www.aepd.es/es/documento/guia-drones-en.pdf> [04.09.2023].

[19] The UK Civil Aviation Authority, The Drone and Model Aircraft Code - For Flying Drones, Model Aeroplanes, Model Gliders, Model Helicopters, and other Unmanned Aircraft Systems Outdoors in the Open A1 and A3 Categories, Protecting people's privacy (Points 20 to 25). Published: October 2019, Last updated: January 2023. Point 21, 32, < https://register-drones.caa.co.uk/drone-code/the_drone_code.pdf> [04.09.2023].

[20] Aerialworx, The GDPR (General Data Protection Regulation) and Drones, 2018, <https://aerialworx.co.uk/gdpr-and-drones/> [04.09.2023].

Additionally, any data beyond the scope of the intended processing and with no need to store, should be promptly deleted.[21]

2.3. Data Security Requirement

Article 17 of the Law of Georgia "On Personal Data Protection" outlines the obligation of data security. Specifically, it states that "the data controller is obliged to implement organizational and technical measures to ensure the protection of data from accidental or unlawful destruction, alteration, disclosure, extraction, or any other form of unlawful processing, as well as from accidental or unlawful loss." Various security challenges may arise during data processing using drones. Therefore, it is the responsibility of the drone operator to implement appropriate safety measures.

First of all, it is important to determine if the drone is connected to any other systems. In such a case, appropriate safety measures should be taken. In addition, the drone operator must ensure that all data collected is stored securely, which may be achieved by encrypting the stored information or employing other methods to restrict access to it. This is particularly important when the drone is flown over long distances, beyond the pilot's field of vision, or in the event of a drone crash, which increases the risk of both the device and its data being lost or stolen.[22]

It is the responsibility of the data controller to take the necessary technical and organizational measures to ensure the security of data processing using drones. Therefore, the data controller should pay special attention to the technical features that the drone is equipped with and which aim to ensure safety in the process of data collection and storage. Among these considerations, the drone operator should verify where the photo/video material captured by the drone is stored—whether it's on the device itself, a portable memory card, or in a cloud-based system. To mitigate potential risks, the data controller must implement suitable measures, such as encrypting the data before transmitting it to the cloud system.[23]

2.4. "Data Protection By Default and By Design"

Article 26 of the new law of Georgia[24] "On Personal Data Protection" establishes the priority of maximal data protection coverage as the default method automatically employed before considering an alternative approach when developing a new product or service (Data Protection by default and by design), a concept that mirrors Article 25 of the GDPR.

According to this article, considering new technologies, implementation costs, the nature, the extent, context, and purposes of processing, as well as the anticipated risks to the rights and freedoms of the data subject and the principles of data processing, the data

[21] The UK Civil Aviation Authority, The Drone and Model Aircraft Code - For Flying Drones, Model Aeroplanes, Model Gliders, Model Helicopters, and other Unmanned Aircraft Systems Outdoors in the Open A1 and A3 Categories, Protecting people's privacy (Points 20 to 25). Published: October 2019, Last updated: January 2023. Point 25, 33, <https://register-drones.caa.co.uk/drone-code/the_drone_code.pdf> [04.09.2023].

[22] Information Commissioner's Office (ICO), UK, Additional Considerations for Technologies other than CCTV, October 2022, 36-37, <https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-video-surveillance-including-cctv-1-0.pdf> [04.09.2023].

[23] The Data Protection Commission (DPC) of Ireland, Guidance on the Use of Drones, 2022, 5, <https://www.dataprotection.ie/en/dpc-guidance/guidance-on-the-use-of-drones> [04.09.2023].

[24] Law of Georgia "On Personal Data Protection", 3144-XIms-Xmp, 14/06/2023.

controller must take suitable technical and organizational measures (including pseudonymization and/or others) both in determining the means of processing and directly during the processing itself. The adoption of these measures should ensure the effective implementation of data processing principles and the integration of protection mechanisms in the data processing process to safeguard the rights of the data subject. Additionally, the data controller, when determining the volume and extent of data processing, storage periods, and access to data, must ensure that technical and organizational measures are taken to automatically process only the amount of data necessary for the specific purpose of processing. These measures should be implemented in a manner that grants access to only the minimum amount of data automatically to an indefinite number of individuals until an authorized alternative approach is selected. Thus, on one hand, the drone manufacturer must integrate mechanisms that minimize the data collected by the drone during the production process. In producing drones, it is essential for the manufacturer to operate with a foundation of respecting human rights to safeguard the privacy of subjects.[25]

On the other hand, the drone operator must consider data protection issues when selecting the appropriate drone for a specific task, planning the flight route, and developing data processing procedures.[26]

It is the responsibility of the drone operator, as a data controller, to ensure that the drone system he intends to use complies with the high priority data coverage provided for in Article 26 of the Law (ensuring that the drone has technical capabilities such as recording and storing data only when it climbs to a certain height[27] or reducing the clarity/resolution of the photo to the minimum necessary to achieve the purpose of data processing [28] among other measures).

2.5. Data Protection Impact Assessment

According to the first paragraph of Article 31 of the new Law of Georgia "On Personal Data Protection," if during data processing, considering new technologies, the category and volume of data, as well as the purposes and means of data processing, there is a high probability of a threat to the violation of basic human rights and freedoms, the data controller is obliged to conduct a data protection impact assessment in advance. Impact assessment is not a one-time process, rather, it is ongoing, especially when the data processing measure is dynamic and characterized by periodic changes.[29]

Based on the reasoning developed in the previous chapters, it is evident that in many cases, data processing using a drone may reach the thresholds outlined in the

[25] Privacy by Design Guide, Resource for Drone Operators and Pilots, 2019, 6-7.
[26] Ways in Which the GDPR Will Impact the Drone Sector, 2018, <https://dronerules.eu/en/professional/news/5-ways-in-which-the-gdpr-will-impact-the-drone-sector> [04.09.2023].
[27] Information Commissioner's Office (ICO), UK, Additional Considerations for Technologies other than CCTV, October 2022, 37, <https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-video-surveillance-including-cctv-1-0.pdf> [04.09.2023].
[28] Spanish Data Protection Agency, Drones and Data Protection, 2019, 3, <https://www.aepd.es/es/documento/guia-drones-en.pdf> [04.09.2023].
[29] Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing is "likely to Result in a High Risk" for the Purposes of Regulation 2016/679, 2017, 14.

aforementioned article, thereby triggering the data controller's obligation to conduct an impact assessment on data protection.

It should be noted that the responsibility to conduct an impact assessment lies with the data controller. While it is possible for another individual to carry out the assessment, the data controller remains accountable for this obligation.[30]

In the process of assessing the impact on personal data protection concerning the use of drones, attention should be given to the following issues: defining the operational area of the drone; tracking the movement of processed data (which involves a systematic description of the processing procedure); establishing the necessity and proportionality of data processing; identifying potential threats and evaluating their impact; and outlining measures to mitigate or address identified risks.[31] It is crucial for drone operators to incorporate risk-based and risk management strategies into the construction and operation of drones. Before deploying a drone, operators should conduct an analysis of potential threats to personal data protection, this analysis should aim to strike a fair balance between the interests of data subjects and the drone operator.[32] Additionally, factors such as the intended operation's purpose, the type of drone to be utilized, and the technologies integrated into it should be considered during the evaluation process.[33]

It is recommended that experts and stakeholders should be involved in the impact assessment process. Additionally, it's crucial to engage the Personal Data Protection Officer (if applicable) to facilitate a thorough assessment.[34] Furthermore, whenever feasible, it's preferable for the data controller to consult with the data subjects or their representatives during the preparation of the impact assessment. For instance, when using a drone in a populated area, such communication may involve local residents, businesses, neighborhood associations, as well as educational, medical, political, or religious institutions in the vicinity.[35]

The impact assessment on data protection should be perceived as a tool that helps the data controller make informed decisions about data processing[36], which allows them to determine whether the use of a drone is truly necessary and appropriate for achieving a specific goal.[37]

3. Analysis of European Approaches

Across the European Union, regulations outlined by both the GDPR and national personal data protection laws govern the protection of personal data when using drones.

[30] Ibid.
[31] Data Protection Impact Assessment Template, Resource for Ddrone Operators and Pilots, 2019, 3.
[32] *Tarr T., Tarr J.A., Thompson M., Wilkinson D.*, Data Protection, Privacy and Drones, Clyde & Co LLP, 2022, 3.
[33] Spanish Data Protection Agency, Drones and Data Protection, 2019, 5,
<https://www.aepd.es/es/documento/guia-drones-en.pdf> [04.09.2023].
[34] Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing is "likely to Result in a High Risk" for the Purposes of Regulation 2016/679, 2017, 15.
[35] Data Protection Impact Assessment Template, Resource for Drone Operators and Pilots, 2019, 5.
[36] Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing is "likely to Result in a High Risk" for the Purposes of Regulation 2016/679, 2017, 14.
[37] Information Commissioner's Office (ICO), UK, Additional considerations for technologies other than CCTV, October 2022, 36.

However, in addition to these legislative acts, various specialized documents may also address personal data protection issues related to drone usage. These may include manuals prepared by supervisory bodies, internal regulations governing civil aviation, and documents developed by the European Union in this field.

3.1. Regulation (EU) 2019/947 on the Rules and Procedures for the Operation of Unmanned Aircraft

In the European Union exists regulation concerning the rules and procedures for operating unmanned aircraft, which outlines specific conditions for the use of unmanned aerial systems, including the relevant personnel, remote pilots, and organizations involved in these operations.[38]

Separate articles of the regulation address personal data protection concern in the operation of unmanned aerial systems. For instance, Article 12, paragraph 2 stipulates that for an individual to receive authorization to operate a drone, they must undergo a successful assessment, which includes a declaration by the drone operator confirming compliance with EU legislation, including regulations on personal data protection. Additionally, the regulation outlines procedures for registering drone operators if the drones they operate are equipped with systems capable of processing personal data.[39]

In addition, the regulation mandates specific obligations for an unmanned aerial vehicle operator as outlined in its annex, according to which operators are required to take appropriate measures to ensure that their planned operations are in compliance with the General Data Protection Regulation (GDPR). This includes the preparation of a data protection impact assessment, which must be conducted upon request from the national data protection authority.

3.2. United Kingdom — Drone and Model Aircraft Code

In addition to personal data protection legislation, the United Kingdom has an active "Drone and Model Aircraft Code"[40], established by the Civil Aviation Authority, with one of its chapters dedicated to safeguarding individuals' right to privacy.

Along with general calls to the need for personal data protection, the code delineates specific responsibilities for drone operators. For instance, to prevent intrusive photo or video recording that egregiously infringes upon people's privacy, operators should possess knowledge about the technical capabilities of the drones they utilize. Specifically, operators should be familiar with the drone's image recording capabilities, including its zoom functionality, and whether it allows for starting and stopping filming during flight. Additionally, the code advises operators to position themselves visibly to data subjects during filming, facilitating their understanding of who is operating the drone. Moreover, the code

[38] EU Regulation 2019/947 on the Rules and Procedures for the Operation of Unmanned Aircraft, 24 May, 2019, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0947> [04.09.2023].
[39] Ibid, Art. 14.5 (a-ii.).
[40] The UK Civil Aviation Authority, The Drone and Model Aircraft Code - For Flying Drones, Model Airplanes, Model Gliders, Model Helicopters, and other Unmanned Aircraft Systems Outdoors in the Open A1 and A3 Categories, Protecting people's privacy (Points 20 to 25). Published: October 2019, Last updated: January 2023, <https://register-drones.caa.co.uk/drone-code/the_drone_code.pdf> [04.09.2023].

emphasizes the importance for data controllers to warn data subjects before capturing photos or videos, ensuring the security of captured media, and refraining from making them public without consent.

3.3. Ireland — Guidance on Data Processing Using Drones

In May 2022, the Irish Data Protection Commission released guidance on data processing using drones.[41] "The manual defines drones as a broad category of unmanned aerial vehicles remotely controlled and outfitted with technology for capturing images, videos, sound, and/or other data, which are subsequently transmitted to smart devices such as cloud storage. Drones have the potential to transform into mobile surveillance systems and process the personal data of individuals passing by, who are considered data subjects."[42]

Accordingly, the Irish supervisory authority categorizes drone operators as data controllers, except when the drone is solely for domestic or personal use and imposes specific obligations on them to prevent irreversible infringement of data subjects' rights. Additionally, it's worth noting that "the guidelines do not cover the use of drones for law enforcement purposes."[43]

According to the guidelines, "when a data controller utilizes a drone and it is not solely for personal or household use, they are obligated to demonstrate that:

- data processing was in the interest of the data subject;
- The use of the drone is necessary to achieve the intended legitimate purpose;
- that it does not have a disproportionate impact on the data subject.

In addition, it is noted that the supervisory body, depending on a number of circumstances, may require data controllers to assess the impact of data processing and develop a privacy policy document. Moreover, data controllers must take into account:

- Their actions must comply with the laws governing the operation of drones (for example, trespassing on private property);
- They must define the initial and subsequent purposes of the data processing;
- In case of an information request from the data subject, they must provide comprehensive information about the purposes of data processing, legality, and rights of the subject;
- Data processing must be based on a legal basis;
- In the process of data processing, they must consider the principle of data minimization, the possibility of depersonalization, and pseudonymization to avoid untargeted (excessive) data processing".[44]

"In the case of using a drone for household and economic purposes, the supervisory body advises drone operators to adhere to the "principle of reasonableness" when determining the scope of data processing. They should avoid filming faces and intruding into other people's private spaces."[45]

[41] The Data Protection Commission (DPC) of Ireland, Guidance on the Use of Drones, 2022, <https://www.dataprotection.ie/en/dpc-guidance/guidance-on-the-use-of-drones> [04.09.2023].
[42] Personal Data Protection Service, Worldwide Practice, June/2022, 11-12. <https://personaldata.ge/ka> [04.09.2023].
[43] Ibid, 12.
[44] Ibid.
[45] Ibid.

3.4. Spain — Guidance on "Drones and Data Protection"

In May 2019, the Spanish Data Protection Agency released a guide titled "Drones and Data Protection." This guide is designed to offer drone operators further insights and recommendations concerning issues related to personal data protection.[46]

The document states that the general obligation to comply with the provisions of data protection is determined by Article 26 of the Royal Decree No. 1036/2017, on the Regulation of the Civilian Use of Aircraft by Remote Control. However, it should considered that together with the legislation regulating airspace, the conditions established by the GDPR fully apply to data processing by means of drones, regardless of whether the drone is used for professional or recreational purposes.

The guidelines delineate between two categories of data processing arising from drone usage. Firstly, instances where the drone's intended purpose inherently involves the necessity for data processing (e.g., video surveillance). Secondly, scenarios where the drone's purpose doesn't inherently entail a requisite need for data processing (e.g., infrastructure inspection, topographical measurements, etc.), although depending on circumstances, may impact individuals' rights to data protection and privacy.

The guidelines offer precise recommendations for drone operators, such as:

- To minimize data, operators should reduce the number of individuals and identifiable objects within the frame, like license plates. This objective can be accomplished by scheduling flights during periods of low human activity in a designated area;
- Additionally, to minimize data, operators should conduct video/audio recording and/or photography only during specific moments when necessary, rather than throughout the entire flight;
- Operators must utilize data protection measures integrated into the drone, such as reducing the resolution of photos to the minimum necessary to achieve the purpose of data processing, thereby making data subjects less identifiable;
- In areas where the presence of people is unavoidable, photos should be taken in a manner that prevents the identification of individuals captured in them. For instance, this can be achieved by capturing photos from a sufficient height;
- Unnecessary information related to data subjects should be avoided during storage. For instance, if the purpose of photography is to conduct a topographic survey of the coastline, there is no need to retain photos of people vacationing on the beach.

The guide also offers the following additional recommendations:

- For installation on a drone, the most suitable technologies for the intended purpose should be selected;
- Mechanisms should be implemented to ensure proper notification of data subjects;
- To create the necessary security guarantees for the protection of data subjects' rights, appropriate technical and organizational measures should be implemented. It is particularly important to avoid the risk of unauthorized data processing during the transfer of collected data;

[46] Spanish Data Protection Agency, Drones and Data Protection, 2019, <https://www.aepd.es/es/documento/guia-drones-en.pdf> [04.09.2023].

- Unnecessary personal information should be promptly deleted or depersonalized after data collection;
- The operator must ensure that both the drone and themselves are as visible and identifiable as possible to the data subject.

The manual lists specific steps a data controller must take before using a drone, including:

- The operator must check if national legislation permits the use of the drone and, if required, obtain authorization from the relevant aviation authority. Failure to comply with national laws regarding drone usage could result in data processing during such flights being deemed in violation of the principle of legality outlined in the GDPR;
- Before undertaking any action that unavoidably involves data processing, it is crucial to analyze the necessity for a data protection impact assessment. This determination should consider factors such as the purpose of data processing, the type of drone being used, and the technologies employed.
- If photographs are taken for personal use, it is important not to make them public on the Internet in a form accessible to an indefinite circle of individuals (when such photographic material allows identification of persons);
- It is necessary to assess in advance the physical safety of the flight and ensure compliance with aviation legislation.

4. Conclusion

The European standards developed around data processing by drones remain essentially similar. Special emphasis is placed on obligations related to transparency, informing the data subject, ensuring data security, and practicing data minimization throughout the data processing cycle. Additionally, when developing a new product or service, it's important to consider data protection standards (Data Protection by Design and by Default) and preparation an impact assessment on data protection. Also, it's worth noting that the new law of Georgia "On Personal Data Protection," which main part is set to come into effect on March 1, 2024,[47] imposes a number of obligations, including those directed at drone operators acting as data controllers. Hence, processing personal data in the context of drone usage in compliance with the law and international standards is crucial. Doing so will significantly mitigate the heightened risk of violating the rights of data subjects, stemming from the extensive scale and unique nature of data processed through drone operations.

Bibliography:

1. Law of Georgia “On Personal Data Protection”, 5669-rs, 28/12/2011.
2. Law of Georgia “On Personal Data Protection”, 3144-XIms-Xmp, 14/06/2023.
3. Personal Data Protection Service, World Practice, June/2022, 11-12. <https://personaldata.ge/ka> [04.09.2023].

[47] Law of Georgia on “Personal Data Protection”, 3144-XIms-Xmp, 14/06/2023, Art. 90.

4. Data Protection Impact Assessment Template, Resource for Drone Operators and Pilots, 2019, 3, 5.
5. EU Regulation 2019/947 on the Rules and Procedures for the Operation of Unmanned Aircraft, 2019.
6. Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679, 2017, 14-15.
7. Information Commissioner's Office (ICO), UK, Additional Considerations for Technologies other than CCTV, 2022, 36-37.
8. Spanish Data Protection Agency, Drones and Data Protection, 2019, 1, 3-5. <https://www.aepd.es/es/documento/guia-drones-en.pdf> [04.09.2023].
9. *Tarr T., Tarr J.A., Thompson M., Wilkinson D.,* Data Protection, Privacy and Drones, Clyde & Co LLP, 2022, 1, 3.
10. The GDPR (General Data Protection Regulation) and Drones, 2018, <https://aerialworx.co.uk/gdpr-and-drones/> [04.09.2023].
11. The Data Protection Commission (DPC) of Ireland, Guidance on the Use of Drones, 2022, 4-5, <https://www.dataprotection.ie/en/dpc-guidance/guidance-on-the-use-of-drones> [04.09.2023].
12. The UK Civil Aviation Authority, The Drone and Model Aircraft Code - For Flying Drones, Model Aeroplanes, Model Gliders, Model Helicopters, and other Unmanned Aircraft Systems Outdoors in the Open A1 and A3 Categories, Protecting people's privacy (Points 20 to 25), October 2019, Last updated: January 2023, Point 22, 32-33, <https://register-drones.caa.co.uk/drone-code/the_drone_code.pdf> [04.09.2023].
13. Privacy by Design Guide, Resource for Drone Operators and Pilots, 2019, 6-7.
14. Ways in Which the GDPR Will Impact the Drone Sector, 2018, <https://dronerules.eu/en/professional/news> [04.09.2023].

Tinatin Lolomadze*

Personal Data Protection According to the "Three-step Test" of the European Court of Human Rights: Risks and Challenges

Data protection is a key aspect of the legislative space. Data protection protects personal information Privacy and security in the face of technological advances and increased data usage.

The article discusses the practice of the European Court of Human Rights and the "three-step" test, which is a widely recognized principle, and is used to assess the legality and validity of restrictions on fundamental rights. The "three-step" test requires that any limitation of a right, such as the right to data protection, must meet three criteria: legitimacy, necessity and proportionality. By following a three-step test, legislators and judges can strike a balance between protecting data privacy and a legitimate purpose or interest.

Keywords: *Data protection, Protection of human rights, Basic regulation of data protection, Right to private life, Legitimacy.*

1. Introduction

Every person has a personal life, it is the space that gives us the opportunity to develop as individuals and become a part of society. It is not surprising that we often want our private lives to be hidden from the public eye. This does not necessarily mean that, as if, by keeping the existing information, we are committing a crime. In fact, this is absolutely harmless information that concerns a person's religious, political or social views. Private life is the actual essence of privacy, and the disclosure of information should depend on the individual and his or her desire. It is the privacy and protection of personal life that gives people the opportunity and courage to be able to express their opinion. It also guarantees to the state that one's personal information, thoughts, views and opinions remain free from judgment. One aspect of the right to privacy is the protection of personal data, which is considered a basic human right in today's democratic states. To date, a number of important legislative and institutional reforms are being implemented to realize this right. The European Court of Human Rights explains that the right to the protection of personal data is not an autonomous right, but is included among various Convention rights and freedoms[1]. The court recognized that the protection of personal data is of fundamental importance for the enjoyment of the

* Master of Law, PhD student of the Faculty of Law at Ivane Javakhishvili Tbilisi State University.

[1] *Amann v. Switzerland,* Application №27798/95, European Court of Human Rights, February 16, 2000, §65.

right to respect for private and family life and correspondence, as guaranteed by Article 8[2] of the Convention. In the digital age, the safeguarding of personal data has become an urgent issue worldwide. For example, a robust data protection framework, such as the General Data Protection Regulation (GDPR), has been established. An essential aspect of understanding and implementing these regulations is compliance with human rights principles.

The article aims to explore the relationship between data protection regulations and the three-step test established by the European Court of Human Rights (ECtHR). By analyzing this test, we will explore how states should regulate database protection to ensure individual rights and protect people from potential risks. By examining the interplay of rights, risks and regulations, the importance of striking a delicate balance between privacy and legitimate public interests in the digital age will be assessed.

2. Protection of Personal Data by the European Court of Human Rights

Data protection plays an important role in protecting an individual's enjoyment of private and family life, as it prevents the public disclosure of personal information. The collection, storage and disclosure of data constitutes an invasion of privacy. Article 8 of the European Convention on Human Rights recognizes both the right to personal data and the right to private and family life, residence and correspondence. Although the protection of personal data and the protection of privacy are different concepts, both of them seek to protect human autonomy and dignity[3]. The right to protection of personal data is a modern and relevant aspect of privacy rights aimed at ensuring the proper processing and development of personal information. The privacy principle covers a wide range of subjects, including sensitive and personal details, and aims to prevent any arbitrary interference.[4]

According to Article 1 of the European Convention on Human Rights, states have an obligation to "ensure" Protection of rights and freedoms provided for by the Convention. This obligation implies not only the prevention of violations of rights and freedoms (negative obligation), but also the active protection of personal safety, even when violations are carried out by third parties (natural and legal entities) (positive obligation) [5]. Although the primary objective of many provisions of the European Convention is to prohibit unjustified restrictions on public human rights, there is no doubt that states are responsible for ensuring the effective protection of these rights. The European Court of Human Rights has held that a positive obligation derives from the provisions of the Convention, including Article 8, which protects personal and family rights. In the case of: Marx v. Belgium, the European Court emphasized that the essential purpose of this provision is to protect individuals against arbitrary interference by public authorities. The role of the state goes beyond merely refraining from intervention; It also requires "respect" for family life. Thus, the protection of personal data implies the intervention of the national state and the legal framework and the practical

[2] *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland,* Application №931/13, European Court of Human Rights, June 27, 2017, §137.

[3] Guide to Article 8 of the Convention - Right to Respect for Private and Family Life, European Court of Human Rights, 2022.

[4] Guide to the Case Law of the European Court of Human Rights/Data Protection, Council of Europe/European Court of Human Rights, 2022, 7.

[5] *Korkelia K.,* Towards the integration of European standards: The European Convention on Human Rights and the Experience of Georgia, Tbilisi, 2007, 14-15 (in Georgian).

implementation of data protection measures. It is important to note that although Article 8 focuses primarily on the protection of private life, privacy as a fundamental element appears in private life itself. Confidentiality, in the context of personal data, is a crucial aspect of maintaining an individual's privacy. Ensuring the confidentiality of personal information through data protection mechanisms is a key factor in protecting the right to privacy and maintaining the necessary level of confidentiality and trust in personal relationships and transactions.

When assessing a potential violation of a person's right to data protection, it is crucial to refer to Article 8, paragraph 2, which outlines the prerequisites for legitimate interference. According to this provision, any interference must meet three criteria: it must be "necessary in a democratic society", "in accordance with the law", and must serve a "legitimate purpose". The requirement of interference, "in accordance with the law", implies that any limitation of the right to data protection must be based on clear and predictable legal provisions. This ensures that individuals have reasonable expectations of how their personal data will be processed and protected. In addition, the interference must have a “legitimate aim. This means that, through data processing, the invasion of a person's private life must have a justified purpose. Examples of legitimate purposes include national security, public safety, crime prevention, health protection, or the rights and freedoms of others. Finally, intervention must be considered "necessary in a democratic society." This criterion requires a balance between the competing interests of data protection and other public considerations. It requires that the interference be proportionate, meaning that it must be the least intrusive measure to achieve the legitimate aim pursued. of necessity the test also includes consideration of alternative means of achieving the same objective which would have less impact on the individual's right to data protection. Incorporating these criteria, Article 8(2) establishes a framework for assessing whether an interference with the right to data protection is justified and complies with human rights standards.

3. Compliance with the Law

Restrictions on the right to personal data protection must be regulated by law. This requirement implies that the restriction must have a legal basis that is accessible, foreseeable and formulated with sufficient clarity, which gives a person the opportunity to understand their duties and regulate their actions. The legal basis must clearly define the scope and form of exercise of authority by the relevant authority, which protects individuals from arbitrary interference.[6] In order for the intervention to be in accordance with the law, there are several prerequisites :

- There must be legislation in the state to process personal data;
- The legal basis requires that the processing of personal data is"necessary". If the State can reasonably achieve the same purpose without the processing, then the processing of the data is unlawful;
- The lawful basis for processing must be established prior to data collection;
- The purpose of data processing must not be changed to another legal basis at a later date, unless the reason for the change is justified;

[6] Necessity Toolkit - European Data Protection Supervisor, Necessity Toolkit, Brussels, 2017, 4.

- If a special category of data is subject to processing, both the legal basis for general processing and additional conditions for the processing of this type of data must be defined.[7]

The European Court of Human Rights considered whether personal data undergoing automatic processing must be received and processed fairly and lawfully, as provided for in the "Protection of Individuals with regard to Automatic Processing of Personal Data " (so-called Convention 108) of the Convention - in Article 5, then violation of Article 8 due to lack of legal basis. For example , in the case of Taylor-Sabor v. United Kingdom, the applicant was subject to police surveillance of his pager, and the legislative space did not provide for the control of information obtained as a result of the surveillance of pager messages[8]. The case of M.D. is similar. MD and others v. Spain, where the Court noted that, on the one hand, there was no domestic legal provision justifying the police action, and on the other hand, there were no guidelines. The court found that the police report of the judges and Magistrates' personal data, photos and political Disclosure of views was not provided for by the law and violated Article 8[9]. In other cases, the court found a violation of Article 8 because Domestic laws for the protection of personal data were either unavailable or confidential or not transparent. for example , in the cases of Vasil Vasilev v. Bulgaria and Nuh Uzun and others v. Turkey,[10] the Court established such issues as: Limited access to laws governing personal data or insufficient clarity of regulations[11]. In contrast, in Ben Faiza v. France, where the domestic law was clear, transparent and adequately safeguarded against potential Against violence, the court did not find a violation of Article 8[12]. In addition, the Court emphasizes that in cases involving covert surveillance measures, such as wiretapping, it is important to have clear and detailed rules to avoid arbitrary interference. The law should provide citizens with sufficient guidance on the circumstances and about the conditions under which state bodies can use the above measures. The Court noted that the law must indicate the scope of any discretion granted to the competent authorities and show the ways of its implementation with sufficient clarity so that subjects can adequately protect themselves from arbitrary interference.

Judicial practice also outlines specific elements that must be considered in the legislation regarding hearings, for example: defining the nature of offenses, specifying the categories of person's subject to hearing, establishing time limits and also data verification and storage procedures, and implementing security measures.

Regarding the collection and storage of personal data by the authorities for the purpose of preventing or punishing crime, case law emphasizes the need for clear and detailed rules, eg: in the case of Cathy v. United Kingdom, the Court explained that the collection of data was subject to the domestic legal framework, but the Court also distinguished that the data collection did not have a clearer and more understandable legal basis. The court noted that "domestic extremism " is interpreted differently by different agencies. Thus, it was unclear to the court, based on what criteria information about the citizen was collected. In the

[7] Guide to the General Data Protection Regulation (GDPR), Information Commissioner's Office, 2022, 19.
[8] *Taylor-Sabori v. the United Kingdom,* Application №47114/99, European Court of Human Rights, October 22, 2002, §19.
[9] *MD and Others v. Spain,* Application №36584/17, European Court of Human Rights, September 28, 2002, §§ 61-64.
[10] *Nuh Uzun and Others v. Turkey,* Application №49341/18, European Court of Human Rights, September 5, 2022, §§ 80-99.
[11] *Vasil Vasilev v. Bulgaria,* Application №7610/15, European Court of Human Rights - August 16, 2022, §§ 169-170.
[12] *Ben Faiza v. France,* Application №31446/12, European Court of Human Rights - May 8, 2021, §§ 58-61.

mentioned case, the court discussed not only the collection of data, but also their storage, the court pointed out that the domestic legislation did not provide for the maximum period of data storage. In addition, the applicant was not a threat to anyone (he was 95 years old), the records collected reflected the applicant's political views, which represented a special kind of data. Therefore, they were subject to high standards of protection. It was the sensitive nature of the data that represented the main essence of the case, on which the Court expressed its opinion: "When the powers granted to the state are vague, which creates a risk of arbitrariness, and when technologies are constantly developing and improving, it is important to check the compliance with the principles of Article 8 of the Convention." According to the court, the applicant had the right to request the erasure of the data, although there were no properly constituted procedural guarantees of data protection. The domestic legal framework stipulated that the data was kept for at least 6 years. Then the need to keep them was reviewed and evaluated. The case did not show whether the data was reclassified or not. The court noted that there should have been a maximum retention period for the data, in addition, the police had more information than was necessary, and the relevant agencies did not take into account the sensitive nature of the data.[13] In its decisions, the court emphasizes the importance of rules governing the duration, storage, use, access and destruction of such data, protecting their integrity and confidentiality.

4. Legitimate Purpose

In violation of Article 8, a legitimate purpose must also be established, which means that the personal data during the automatic processing must be collected for clear, specific and legitimate purposes. In these cases, the examination of legitimate aims that might justify interference with the exercise of Article 8 rights as enumerated in paragraph 2 is quite limited. The purposes of legitimate interference are: 1. National security, 2. Public safety and protection of the economic welfare of the country, 3. Prevention of disorder or crime, 4. Protection of health and morals or protection of the rights and liberties of others. The existence of one or more of these purposes, asserted by the Government, must also be shared by the Court under Article 8(2) to implement the objectives of the clause[14].

for example , the court found that the transfer of bank data to the authorities of another country based on a bilateral agreement served a legitimate purpose, as it contributed to the protection of the country's economic well-being[15].

Referring to international instruments that emphasize fairness and equal opportunities in the fight against doping, the Court found that the protection of health and morals justified the obligation to locate athletes in order to combat doping. In sports, the court linked this kind of action to what the government called "morality" with the legitimate aim of protecting the rights and freedoms of others , since the presence of doping agents encouraged amateur athletes, especially young people, to follow them [16]. It was determined that listening to the

[13] *Catt v. United Kingdom,* Application №43514/15, European court of Human Rights, January 24, 2019.
[14] Guide to Article 8 of the Convention - Right to Respect for Private and Family Life, European Court of Human Rights, 2022, 12.
[15] *GSB v. Switzerland,* Application №28601/11, European Court of Human Rights December 22, 2015, § 83.
[16] *National Federation of Sportspersons' Associations and Unions (FNASS) and others v. France),* Application №48151/11, №77769/13, European Court of Human Rights January 18, 2018, §§ 164-166.

telephone conversations of the director of the prison suspected of corruption, saving this information and disclosing it was aimed at preventing corrupt actions, ensuring transparency and openness in the public service. Thus, the legitimate aims were to prevent disorder or crime and to protect the rights and liberties of others [17].

In each case, the Court has consistently recognized the existence of one or more legitimate goals pursued by governments. These findings highlight the Court's obligation to balance the protection of personal data with the need to protect the legitimate interests of society.

5. Necessary in a Democratic Society

In order for any measure that interferes with the protection of personal data under Article 8 to be considered necessary in a democratic society, it must meet the criteria of pressing social need and must not be disproportionate to the legitimate aims. The reasons given by the government must be relevant and sufficient. Although the initial assessment is made by the national authorities, the final assessment of the need for intervention is subject to judicial review to ensure compliance with the requirements of the Convention. When it comes to the violation of rights, the court considers whether the legislation adopted by the state provides adequate protection of these rights.

Overall, in order to determine whether a measure to interfere with the protection of personal data is justified under Article 8 in a democratic society, the matter must be considered by the Court in accordance with the requirements of Article 5 of Convention 108.

The Court emphasizes the need for measures to intervene in the protection of personal data in order to maintain proportionality in the face of pressing social needs. It is the role of the Court to consider and assess the necessity of such intervention in the light of national assessments of whether it is consistent with the requirements of the Convention.

5.1. Collected or Recorded Data Minimization Request

Only those data that are "relevant and the volume does not exceed the purpose for which they were collected and/or processed" must be processed. The categories of data selected for processing must be necessary to achieve the stated purpose of the processing operations, and the processor must be strictly limited to collecting only those data that directly fit a specific purpose. The processing of personal data must be proportionate to the legitimate purpose served by the processing. At all stages of data processing, there must be a fair balance between all relevant interests. This means that " adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')".[18]

For example, according to the EU General Data Protection Regulation, the data collected must be: Adequate-enough to properly fulfill the intended purpose; relevant - to have a rational connection with this goal; Be limited to what is necessary - no more information than necessary should be stored.

[17] *Adomaitis v. Lithuania,* Application №14833/18, European Court of Human Rights, January 18, 2022, § 84.
[18] General Data Protection Regulation, Article 5 (1) (c).

Therefore, the minimum amount of personal data necessary to fulfill the purpose should be determined. But the question arises, how to understand what is adequate, appropriate and limited? Legislation will not be able to define these terms. However, this will obviously depend on the purpose of collecting and using the personal data. It can also vary from one individual to another. So , in order to assess whether the " right amount " of personal data[19] is stored , it is first necessary to find out the relevant purpose and the nature of the data . in his own practice as well.

For example, the court found a violation of Article 8 after the retention of information obtained from electronic devices seized during the search was not relevant to the case. Also, it did not appear that any kind of selection procedure was performed to minimize the amount of these data [20]. The court considered whether the automatically processed personal data were suitable, relevant and not excessive for the purposes for which they were recorded in various instances. In some cases, the Court found a violation of Article 8 of the Convention. These violations occurred because no procedures were followed to minimize the amount of data seized from the applicants' electronic devices during searches. The court's decision to publicly identify a non-participant (involved in a case of sexual harassment at the workplace), without protecting confidentiality, was considered unnecessary and potentially stigmatizing. In addition, the disclosure of personal data captured without the journalist's consent in the progress report of the investigation was considered excessive and pointless.[21]

According to the court, databases should not be designed to maximize the information to be stored in order to prevent and punish for a crime. The argument that storing more data leads to crime prevention does not justify storing information on the entire population, including deceased relatives, which is clearly excessive and inappropriate. The Court, in accordance with legitimate purposes, emphasizes the importance of adequate, appropriate and proportionate processing of personal data. Excessive retention and disclosure of data, without adequate safeguards, violates the rights and freedoms protected by Article 8 of the Convention. States need to strike a balance between the benefits of data retention and respect for individual privacy.[22]

5.2. Data Accuracy and Update Request

In accordance with EU and Council of Europe legislation, data subjects have the right to request the rectification of their personal data. Their accuracy is necessary to protect data subjects' personal information at a high level. [23]False or incomplete personal data collected and protected by the authorities may complicate the daily life of the subject of personal data protection, or may remove certain statutory procedural guarantees needed to protect the rights of the individual. Such data may be shared between different authorities, which may harm the personal or professional life of the data subject. It is the task of the authorities to verify the accuracy of the stored data. The Court of Human Rights has heard a number of

[19] Guide to the General Data Protection Regulation (GDPR), Information Commissioner's Office, 2022, 27.

[20] *Krugulov and others v. Russia,* Application №11264/04, European Court of Human Rights February 4, 2020, §123-138.

[21] *Khelili v. Switzerland,* Application №16188/07, European Court of Human Rights, October 18, 2011, § 62.

[22] Guide to European Data Protection Law, 2018, 144.

[23] General Data Protection Regulation, Article 16.

cases concerning the government's retention of data that was found to be inaccurate or whose accuracy was disputed by the data subject. Case law shows that data should be kept no longer than to fulfill the purpose for which they were obtained. In the case of S.And Marper v. United Kingdom[24], the Court noted that the permanent storage in a national database of the fingerprints, cellular samples and DNA profiles of persons accused but not convicted of a crime, regardless of the nature or seriousness of the crime of which the person was initially suspected, violates Article 8. for example, in the case of Anchev v. Bulgaria, where the applicant was subject to three investigations and, based on the archive, was "labeled" as a former employee of the security services. All this happened under a law aimed at exposing public officials who collaborated with the communist regime. However, the court dismissed the applicant's complaint, as he was given the right to access the archives and could later challenge the accuracy of the information. It is important to note that the court's decision in this case was specific to the circumstances presented. The Court recognized that providing the applicant with access to the archives and the opportunity to challenge the accuracy of the information was an appropriate remedy given the particular circumstances and the applicant's ability to present specific grounds for his appeal. Overall, this case highlights the importance of ensuring that people have the opportunity to review and challenge information held about them, particularly when it has the potential to affect their reputation and rights. Granting access to relevant archives enables authorized persons to present evidence to challenge the accuracy of such information, which is an important aspect of protecting their rights under the Convention.[25] Practice shows that the authorities must determine the accuracy of the stored data. Storing false or disputed information can have a detrimental effect on the data subject's daily life, reputation and procedural rights. It is very important that the authorities take care to ensure that data storage complies with the principles of accuracy and privacy of individuals, the latter of which is guaranteed by Article 8 of the Convention.

5.3. Limiting the Duration of Personal Data Storage (Requirement that Data Be Kept for No Longer than the Purpose for Which it Was Collected)

In several cases, the court considered the issue of limiting the duration of personal data storage. The court negatively evaluates the storage of data for an indefinite period, and, in addition, the period of data storage largely depends on the severity of the crime. The issue of permanent custody is particularly serious when it comes to minors because of their vulnerable situation, the importance of their development and integration into society [26]. for example , the court found a violation in the case of MK v. France, where the applicant was accused of book theft, but not convicted, and his prints were kept indefinitely [27], on the contrary, in the case - Martens v. Germany, the court declared the case, in which the personal

[24] *SS. and Marper v. the United Kingdom,* Application № 30562/04 and 30566/04, European Court of Human Rights, December 4, 2008, §§ 70-75.
[25] *Anchev v. Bulgaria,* Application №38334/08 - 68242/16, European court of Human Rights, December 5, 2017, §§ 112-115.
[26] Guide to the Case Law of the European Court of Human Rights/Data Protection, Council of Europe/European Court of Human Rights, 2022, 29.
[27] *MK v France,* Application № 19522/09, European Court of Human Rights, April 18, 2013.

data of the applicant was kept indefinitely, clearly unfounded, but the legislation called for reviews at regular intervals of no more than ten years to determine whether data was being retained. The duration is not necessarily decisive in relation to the retention period of the biometric data of convicts, the Court stated that the absence of a maximum period of data retention does not automatically violate Article 8. However, in such cases, procedural safeguards become crucial to ensure that the duration of data retention remains proportionate. Diligence by authorities in assessing and periodically reviewing the need to retain personal data becomes essential to maintain a balance between legitimate objectives and individuals' right to privacy. The duration of storage should depend on the degree of severity of the crime, the past actions of the accused, the strength of the suspicion that exists against the subject, these factors should be evaluated by the state and the proportionality of the storage should be determined in each case, taking into account the purpose of data storage and the nature and severity of the circumstances .[28]

The Court of Justice recognizes that there may be justified reasons for retaining personal data beyond a certain period, especially in cases involving serious crimes , however, the permanent retention of data relating to persons who have not been convicted of any crime, regardless of their age or suspicious nature, is incompatible with Art. 8 at the knee. Procedural safeguards and diligent oversight must be put in place to secure data.

5.4. Request to Restrict the Use of Data for the Purpose for Which They Were Recorded

Importantly, the requirement to limit the use of data to the purpose for which it was recorded is a recurring theme in court practice. The court emphasized the need for strict adherence to this principle in order to protect an individual's right to privacy. A few notable cases provide additional information on this requirement [29]:

For example, in the case of Karabeoglu v. Turkey, the Court found a violation of Article 8 because data obtained from wiretapping during a criminal investigation was used for another purpose, in a subsequent disciplinary investigation. The court emphasized that the use of data for purposes other than those that justified their collection may be a violation of the right to privacy [30]. The case of Surikov v. Ukraine concerned the long-term storage, dissemination and use of data about an individual's mental health for purposes unrelated to the original case. The court concluded that such practices constituted a disproportionate interference with the data subject's right to respect for private life. This case highlights the importance of ensuring that personal data is used only for the purposes for which it was originally collected [31].

Any deviation from this principle, e.g., using data for different purposes or improper disclosure, may violate an individual's right to privacy. The implementation of appropriate safeguards and access control is of crucial importance to ensure the protection of personal data and the protection of the rights of individuals under Article 8 of the Convention.

[28] *Peruzzo and Martens v. Germany,* Application №7841/08 and 57900/12, European Court of Human Rights, June 4, 2013, §§ 44-49.
[29] General Data Protection Regulation, Article 5 (1) (c).
[30] *Karabeyoğlu v. Turkey,* Application №30083/10, European Court of Human Rights June 7, 2016, §111-124.
[31] *Surikov v. Ukraine,* Application №42788/06, European Court of Human Rights, January 26, 2017, § 80-96.

5.5. Data Processing Procedures Transparency Request

In a number of cases related to personal data collected and stored by public authorities, the Court held that the authorities had a positive obligation to provide interested parties with an "effective and accessible procedure"[32] so that they could have access to "all relevant information." The subject of personal data has the right to request information about personal identity for discovery, of course, this requirement of transparency has little effect when the other side of the scale is national security information. The practice shows how important it is to make the legislation transparent and concrete in order not to exceed the discretion of the state bodies. In addition, it is emphasized that despite the powers of the state, the collection of personal data, the final assessment is the prerogative of the court, therefore, the court should be familiar with this issue in order not to allow misinterpretation of the law.

6. Conclusion

Respecting the private life of each person is one of the obligations of a democratic state, as it creates the basis for personal growth and development. Privacy is a haven for citizens where they can freely express their opinions, beliefs and identities without any judgment or fear. Respecting an individual's privacy helps to create an environment conducive to self-expression, creativity and the pursuit of individuality. In the context of data protection, the concept of privacy takes on additional importance. Our personal information is constantly collected, processed and shared with other authorities for companies, from online activities to financial transactions. Our digital footprints leave a wealth of data that can reveal details about our lives. Protecting the privacy of individuals in the digital realm is paramount. It ensures that individuals retain control over their personal information and have the freedom to decide how to use, share and store it. Respect for privacy allows individuals to make informed choices and maintain autonomy over their personal data. Furthermore, privacy is not just a matter of individual rights; It is the fundamental pillar of a democratic society. When individuals feel secure in their private lives, they are more likely to engage in open discourse, express diverse opinions, and contribute to the cultural, social, and intellectual fabric of society. States are obliged, first of all, to create such a legal framework that will be able to protect the data of their citizens, in addition, the problem is that the definition of personal data is changing and becoming more multifaceted. That is why there is a need for more involvement of judicial authorities in the aspect of personal data protection.

Data privacy protection is one of the most important issues. By protecting data, you protect individuals from unwarranted intrusions and surveillance. By valuing and protecting privacy, we create an environment that fosters individuality, self-expression, and the pursuit of personal growth.

[32] *Gaskin v. the United Kingdom,* Application №10454/83, European Court of Human Rights, July 7, 1989, § 40-60.

Bibliography:

1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
2. Guide to European Data Protection Law, 2018, 144.
3. Guide to the Case Law of the European Court of Human Rights/Data Protection, Council of Europe/European Court of Human Rights, 2022, 7.
4. Guide to Article 8 of the Convention - Right to Respect for Private and Family Life, European Court of Human Rights, 2022.
5. *Korkelia K.,* Towards the integration of European standards: the European Convention on Human Rights and the experience of Georgia, Tbilisi, 2007, 14-15 (in Georgian).
6. Necessity Toolkit - European Data Protection Supervisor, Necessity Toolkit, Brussels, 2017.
7. *Adomaitis v. Lithuania*, Application №14833/18, European Court of Human Rights, January 18, 2022.
8. *Amann v. Switzerland*, Application №27798/95, Human Rights European the court big of the Chamber of February 16, 2000.
9. *Anchev v. Bulgaria,* Application №38334/08 - 68242/16, European Court of Human Rights, December 5, 2017.
10. *Ben Faiza v. France*, Application №31446/12, European Court of Human Rights, May 8, 2021.
11. *Catt v. United Kingdom,* Application №43514/15, European Court of Human Rights, January 24, 2019.
12. *Gaskin v. the United Kingdom*, Application №10454/83, European Court of Human Rights, July 7, 1989.
13. GSB v. Switzerland, Application №28601/11, European Court of Human Rights, December 22, 2015.
14. *Karabeyoğlu v. Turkey,* Application №30083/10, European Court of Human Rights, June 7, 2016.
15. *Krugulov and others v. Russia*, Application №11264/04, European Court of Human Rights, February 4, 2020.
16. *Khelili v. Switzerland,* Application №16188/07, European Court of Human Rights, October 18, 2011.
17. *MD and Others v. Spain*, Application №36584/17, European Court of Human Rights, September 28, 2002.
18. *MK v France,* Application №19522/09, European Court of Human Rights, April 18, 2013.
19. *National Federation of Sportspersons' Associations and Unions (FNASS) and others v. France,* Application №48151/11, №77769/ 13, European Court of Human Rights, January 18, 2018.
20. *Nuh Uzun and Others v. Turkey,* Application №49341/18, European Court of Human Rights, September 5, 2022.
21. *Peruzzo and Martens v. Germany,* Application №7841/08 and 57900/12, European Court of Human Rights, June 4, 2013.
22. *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland,* Application №931/13, European court of Human Rights, June 27, 2017.

23. *S. and Marper v. the United Kingdom,* Application №30562/04 and 30566/04, European Court of Human Rights, December 4, 2008.
24. *Surikov v. Ukraine,* Application №42788/06, European court of Human Rights of the Court on January 26, 2017.
25. Taylor-Sabori v. the United Kingdom, Application №47114/99, European Court of Human Rights, October 22, 2002.
26. *Vasil Vasilev v. Bulgaria*, Application №7610/15, European Court of Human Rights, August 16, 2022.

PERSONAL DATA
PROTECTION SERVICE

Address: №7, Nato Vachnadze Str., Tbilisi, 0105
№48, Baku Str., Batumi, 6010
Web: www.personaldata.ge
Tel.: (+995 32) 242 1000
E-mail: office@pdps.ge