GAPS AND CHALLENGES FOR EFFECTIVE JUSTICE FOR PERSONAL DATA PROTECTION AND THE RIGHT TO PRIVACY

Dr. Elena Mujoska Trpevska
Dr. Irena Bojadjievska

September 2023

Funded by the European Union

EU with YOU

This project is implemented by

ЦЕНТАР ЗА ПРАВНИ ИСТРАЖУВАЊА И АНАЛИЗИ
CENTER FOR LEGAL RESEARCH AND ANALYSIS

MYLA

Title:
Gaps and Challenges for Effective Justice for Personal Data Protection and the Right to Privacy

Publisher:
Center for Legal Research and Analysis
Macedonian Young Lawyers Association

For the Publisher:
Lidija Stojkova Zafirovska, CLRA
Aleksandra Cvetanovska, MYLA

Author:
Elena Mujoska Trpevska, Assistant Professor
Irena Bojadjievska, Assistant Professor

Editing:
Center for Legal Research and Analysis

Proofreading and translation:
Dejan Vasilevski

Graphic design:
Vertigo Visual

CIP – Cataloging:

This publication has been created within the project "Effective Justice to Protect the Fundamental Freedoms and Privacy of People in the On-line Space", funded by the European Union. The contents of this publication are the sole responsibility of the authors, and in no way it can be considered to reflect the views of the European Union

Funded by the European Union

This project is implemented by

ЦЕНТАР ЗА ПРАВНИ ИСТРАЖУВАЊА И АНАЛИЗИ
CENTER FOR LEGAL RESEARCH AND ANALYSIS

MYLA

Table of Contents

List of abbreviations

RNM	Republic of North Macedonia
PDPA	Personal Data Protection Agency
LPDP	Law on Personal Data Protection
LEC	Law on Electronic Communications
LEC	Law on Electronic Commerce
OMR	Office for Management of Registers
HIF	Health Insurance Fund
ECtHR	European Court of Human Rights
ECJ	European Court of Justice (Court of the EU)

Executive Summary

Globalization in modern times becomes a factor that has a strong influence on both the emergence of criminal activity and on the phenomenological manifestations it takes. Despite our perception of staying current with the latest advancements, our understanding of globalization as a comprehensive social process needs to be constantly renewed and upgraded. The adoption of international agreements aimed to provide an effective framework for combating contemporary forms of crime, the establishment of national institutional systems, and the coordination of efforts in countering modern, including IT-related, crimes, fall short of solving the issue.

The reason for this is simple: as a country, we fail to address the criminogenic elements within globalization that influence the emergence of criminal activity.

In 2020, the Law on Personal Data Protection was adopted after many years of recommendations that additional efforts should be made to harmonize the national legislation on personal data protection with the General Data Protection Regulation 2016/679 and Directive 2016/680 (EU Progress Reports on RM) and to address the recommendations for strengthening the autonomy and independence of the competent authorities, provided by the group of senior experts on systemic issues of the rule of law relating to the interception of communications revealed in the spring of 2015 (noted in the “Priebe Reports”) and the recommendations to comply with the Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (Expert Opinion – EC).

After the adoption of the Law on Personal Data Protection in August 2021, its full implementation began. The monitoring of the implementation of the Law on Personal Data Protection and the progress and challenges are regularly reflected in the Reports of the European Commission on Chapter 23 – Justice and Fundamental Rights of the National Program for the Adoption of the Law of the European Union (NPAA). This analysis aims to assess the degree of

protection of the right to privacy and free disposal of personal data in the judicial sector, that is, whether the Law on Personal Data Protection comprehensively regulates the issues of collection, storage, transfer and processing of personal data, and especially the principles related to the processing of personal data from the aspect of implementation in practice by judicial authorities. At the same time, there will be an assessment of the competence and identification of inconsistencies of the judiciary and the public prosecution in enabling efficient justice for the protection of human rights, the right to privacy and personal data in the digital space.

INTRODUCTION

Who is responsible for the information published on web pages on the Internet? Is the information adequately processed, secure, and protected? Who bears responsibility for privacy infringements? More specifically, who is liable when the published data is erroneous or lost? What if personal information revealing political views, religious beliefs, or health and sexual orientation data, is exposed?

Privacy, one of the most sensitive aspects of human life, takes various forms, making it one of the most difficult phenomena to fully regulate. In an era marked by rapid internet, ICT, and computer program developments, accompanied by the widespread and unchecked use of social media platforms like Instagram, Facebook, Twitter, TikTok, individuals randomly share personal data, disregarding potential misuse by third parties. Unauthorized intrusions into privacy violate individual autonomy, integrity, and the notion that every person should be free to lead their life as they wish, without undue external influence and decide what information to disclose.[1]

Respecting the rights to privacy and personal data protection promotes democratic values and contributes to the development of a democratic state and society.

Until personally impacted by online or offline privacy breaches or data disclosure without consent, individuals may struggle to grasp the gravity of such infringements. Like many phenomena, we cannot seem to understand it until we experience it ourselves. However, when we find ourselves as victims or affected parties, we immediately seek protection from institutions and judicial authorities.

1 Metamorphosis, Freedom of Expression and Privacy in the Digital Age, December 2014. Source: http://nemrazi.mk/wp-content/uploads/2014/12/Manuel-p--dagogique_mk.pdf.

I.
LEGAL FRAMEWORK

LEGAL FRAMEWORK

1.1 LAW ON PERSONAL DATA PROTECTION

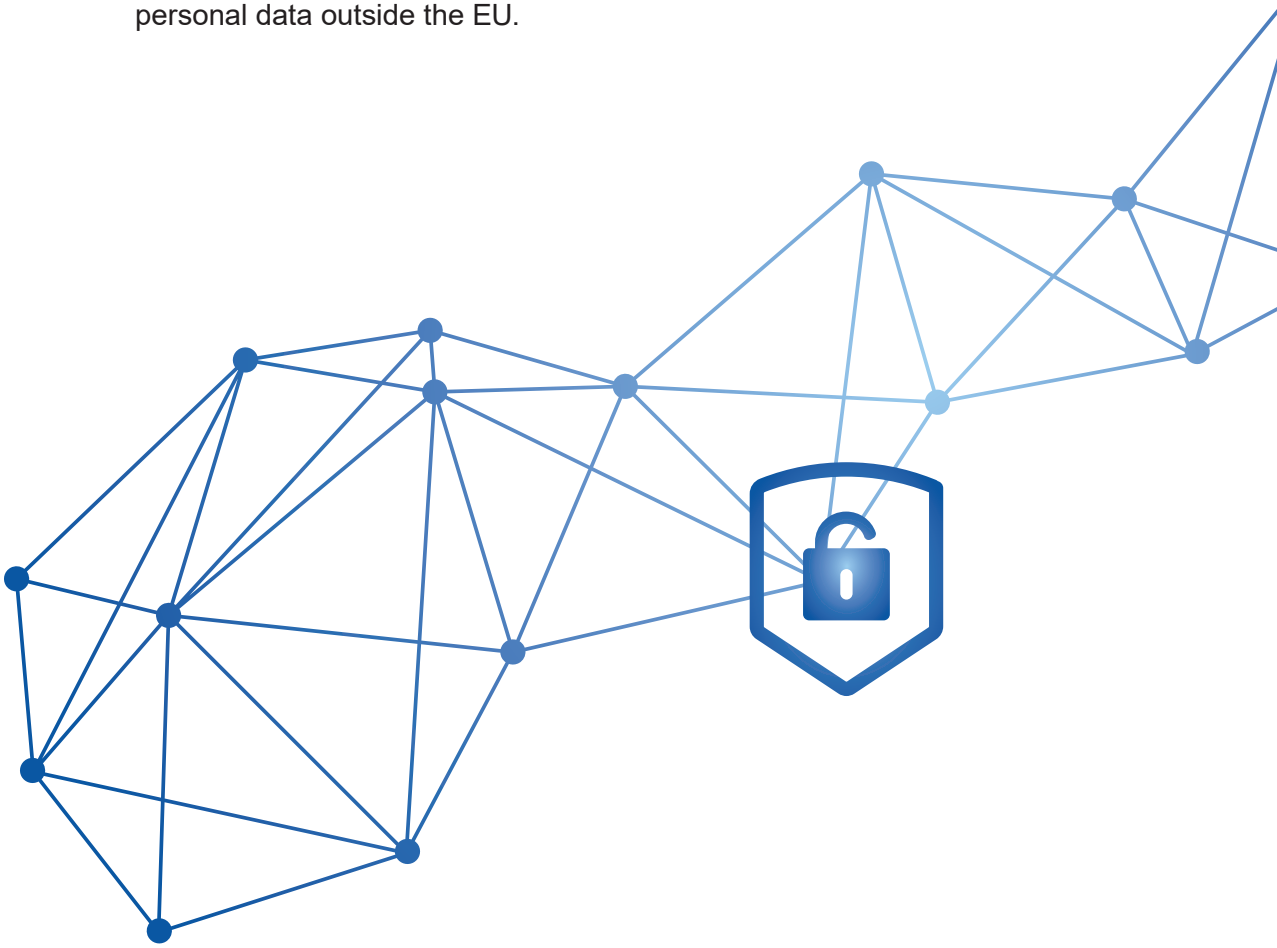
The national legal and institutional framework, which guarantees personal data protection as a fundamental value, is established with the Law on Personal Data Protection[2]. This law, enacted on 16.02.2020, came into effect on 24.02.2020, and underwent its first amendment the following year[3], primarily involving minor technical adjustments and additions. The law transposes the Regulation (EU) 2016/6794 of the European Parliament and the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (CELEX number 32016R0679).[5]

In addition to the foundational law, the Constitution of the Republic of North Macedonia[6] guarantees equality (Article 9), the security and confidentiality of personal data (Article 18), protection against violations of personal integrity arising from registration and processing of information about citizens (Article 18), and the right to privacy (Article 25).

Of the remaining international instruments of the Council of Europe, North Macedonia is a signatory of the European Convention on Human Rights (ECHR)[7] and the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108+)[8] and its protocols[9],

2 Law on Personal Data Protection, Official Gazette No. 42/2020 of 16.02.2020.
3 Law Amending the Law on Personal Data Protection, Official Gazette of RNM No. 294/2021 of 27.12.2021.
4 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). Source: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX-%3A32016R0679.
5 This Directive repeals Directive 95/46/EC, the so-called General Data Protection Regulation.
6 Constitution of the Republic of Macedonia (Official Gazette no. 52/1991; 1/1992; 1/1992; 31/1998; 31/1998; 91/2001; 91/2001; 84/2003; 84/2003; 107/2005; 107/2005; 3/2009; 3/2009; 13/2009; 49/2011; 49/2011; 6/2019 and 6/2019.
7 The European Convention on Human Rights. Source: https://www.coe.int/en/web/human-rights-convention.
8 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108), 28.01.1981. Извор: https://www.coe.int/en/web/data-protection/convention108-and-protocol.
9 Within the Council of Europe, the process of modernizing the existing Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data No. 108 of 1981 has been finalized. Consequently, the new Protocol Amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 223) has been adopted. This protocol brings about modifications to the Convention, both to accommodate new scenarios in the realm of personal data protection and to address advancements in technology applied to data processing.

as well as of the legal framework of the European Union – the Charter of Fundamental Rights in the EU10 and the aforementioned regulation for the processing of personal data, introduced so as the European Parliament, the Council of the European Union and the European Commission strengthen and unify data protection of all natural persons in the EU as well as the transfer of personal data outside the EU.



10 EU Charter of Fundamental Rights on EUR-Lex. Source: https://commission.europa.eu/aid-development-cooperation-fundamental-rights/your-rights-eu/eu-charter-fundamental-rights_en.

INTERNATIONAL LEGAL FRAMEWORK IN THE FIELD OF PERSONAL DATA PROTECTION

The Universal Declaration of Human Rights (Article 1 and Article 12)

All human beings are born free and equal in dignity and rights. They are endowed with reason and conscience and should act towards one another in the spirit of brotherhood. 12. No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks”

European Convention on Human Rights (Article 1 and Article 8)

Everyone has the right to respect for his private and family life, his home and his correspondence. 8. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Charter of Fundamental Rights of the European Union (Article 7)

Everyone has the right to respect for his or her private and family life, home and communications.”

Article 8: “Everyone has the right to the protection of personal data concerning him or her.” 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. Compliance with these rules shall be subject to control by an independent authority.

International Covenant on Civil and Political Rights (Article 17)

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation.
2. Everyone has the right to the protection of the law against such interference or attacks.

UN General Assembly Resolution 68/167

The right to privacy is important for the realization of the right to freedom of expression and to hold opinions without interference, and is one of the foundations of a democratic society.

However, the question remains: is the national legal framework sufficient to contend with the substantial impact of global trends and the rapid development of information technology, along with the emergence of new forms of crime?

With the enactment of the Law on Personal Data Protection, a contemporary concept of a guaranteed right to privacy is established, introducing novel solutions for personal data processing. These include:

- A legal definition of terms related to personal data protection as fundamental freedoms and rights of natural persons, particularly the right to privacy concerning personal data processing.
- A commitment to the principles of accountability and responsibility at both the controller/processor level and the state level.
- Imposition of additional obligations on controllers/processors for establishing the instrument of privacy when designing information systems processing personal data.
- Assessment of the impact of planned data processing processes in relation to personal data protection.
- Establishment of a control mechanism for the Personal Data Protection Agency responsible for personal data protection, to provide input on proposals for any statutory or regulatory frameworks involving personal data processing.
- An obligation to ensure that the Personal Data Protection Agency possess the necessary resources for effective performance of its duties and responsibilities, emphasizing the independence, autonomy and impartiality.

In the broader context of privacy, it embodies the idea of independent action by each individual, free from fear and danger that their actions will be exploited by third parties. Any unauthorized intrusion into this realm of personal privacy constitutes a violation of the person, their dignity and freedom.

While numerous attempts exist to define privacy in the professional literature, the multifaceted nature of privacy leads to the absence of a single definition.[11]

Exemption from free access to information:
Information holders are entitled to decline requests for access to personal data when disclosing such data would constitute a breach of personal data protection.
Article 6, Law on Free Access to Information

The LPDP defines the terms that serve the purpose of the law, including definitions for:

PERSONAL DATA

any information relating to an identified natural person or an identifiable natural person (personal data subject), and an identifiable natural person is a person whose identity can be established directly or indirectly, in particular on the basis of an identifier such as first and last name, personal identification number of the citizen, location data, online identifier, or based on one or more features specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the particular natural person.

DATA CONTROLLER

a natural or legal person, a public administration body, state authority or a legal entity established by the state to exercise public powers, an agency or other body, acting independently or jointly with others, establishing the purposes and the method of personal data processing, and when the purposes and the method of personal data processing is determined by law, the same law establishes the controller or the specific criteria for its identification

11 Sokolovska A., Kocarev Lj., The challenges of the Internet and information technologies: justice, responsibility, privacy. MANU, Articles, 2018, p.138.

DATA PROCESSOR

a natural or legal person, a public administration body, state authority or legal person established by the state to exercise public powers, agency or other body that processes personal data on behalf of the controller

PROCESSING

any operation or set of operations performed on personal data, or a group of personal data, automatically or otherwise, such as: collection, recording, organization, structuring, storage, adaptation or change, withdrawal, consultation, inspection, use, disclosure by transmission, publication or otherwise making available, adjustment or combining, restriction, deletion or destruction

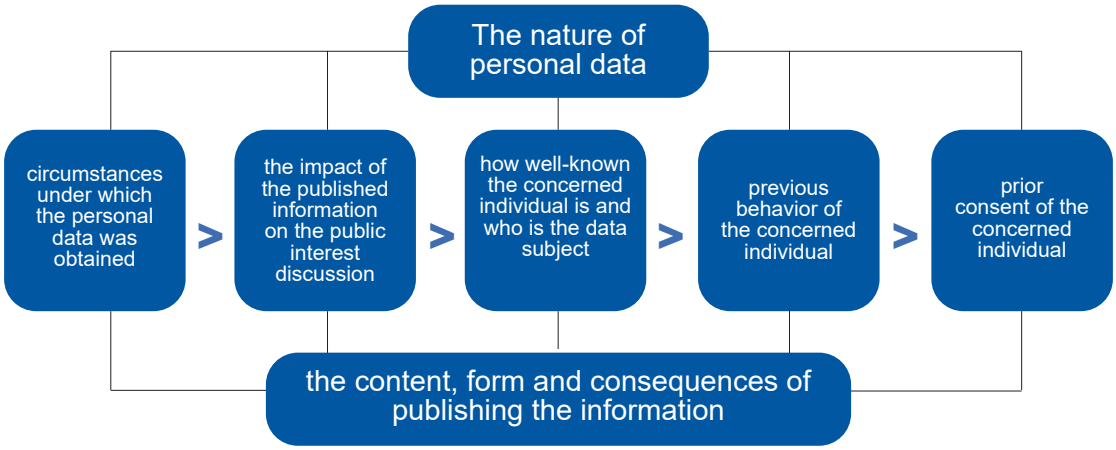
USER

a natural or legal person, a public administration body, state authority or legal person established by the state to exercise public powers, an agency or other body to which personal data is disclosed, regardless of whether it is a third party or not.[12]

Today, citizens have the opportunity to influence and control data holders, personally determining which personal data will be public and which will remain private. Therefore, for the full and effective implementation of legal regulations ensuring personal data protection, public information must be legally regulated.[13]

12 An exception is the situation when state administration bodies and public authorities which may receive personal data in the framework of a particular inquiry in accordance with the law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;, LPDP art. 4 item 9.
13 Metamorphosis: Internet freedom in Macedonia, 2017, p.165..

Additionally, the legal regulation of criteria that balance the right to personal data protection with the freedom of expression and information is of significant importance. Hence, this process[14] pays particular attention to:



Balancing actually represents a derogation from the right to protection of privacy when it comes to the processing of personal data for journalistic purposes or for the purposes of academic, artistic or literary expression[15], but only if the public interest prevails over the private interest of the data subject (Art. 81 paragraph 3 LPDP). Exemptions and derogations from the protection of the right to privacy and the balancing between personal data and the right to information apply in particular to the processing of personal data in the audio-visual field and in news archives and press libraries (Art. 81 paragraph 2 LPDP). The purpose of this article is to ensure greater protection of the privacy of data subjects when their data is processed for the purposes of professional journalism, and the main intention is to ensure the prior consent of the data subject. This wording shows that the "privileged" position of journalists does not mean that they should not respect the principles of personal data protection; instead, they must discern when the public interest outweighs the individual's private interests.[16]

14 Art. 81 para. 4 of the Law on Personal Data Protection, Official Gazette No. 42/2020.
15 In addition to these grounds, the provisions of Chapter II (Principles), Chapter III (Rights of the Data Subject), Chapter IV (Data Controller and Processor), Chapter V (Transfer of Personal Data) and Chapter VI (Personal Data Protection Agency), as well as the provisions of Chapter VII (Special Operations of Personal Data Processing) may be excluded or derogated from if it is necessary to strike a balance between the right to personal data protection and the freedom of expression and information, art. 81. para. 4 of the Law on Personal Data Protection, Official Gazette No. 42/2020.
16 Metamorphosis: Internet freedom in Macedonia, 2017, p.166-167. Link: https://metamorphosis.org.mk/wp-content/uploads/2018/09/dad6a750-e7c6-486f-b061-5d59a0f2eabb.pdf.

The data controller guarantees that they respect the principles of personal data protection , i.e. that:

- it is processed in accordance with the law;
- it is collected for specific, clear and legally defined purposes;
- it is processed in a manner consistent with those purposes;
- it is adequate, relevant and not excessive in relation to the purposes for which it is collected and processed;
- it is accurate, complete and updated as necessary, deleting or correcting data that is incorrect or incomplete; and
- is kept in a form that allows the identification of the data subject no longer than is necessary to fulfill the purposes for which the data was collected for further processing.
- processed lawfully, fairly and in a transparent manner in relation to the data subject ("lawfulness, fairness and transparency")

Personal data protection is guaranteed to every natural person without discrimination based on any personal characteristic or assumption (Article 5 LPDP). This consent should be freely given, specific, informed and unambiguously expressed through a statement or a clearly confirmed action, for the purposes of the processing of their personal data (Article 4 item 11 LPDP).

The Law on Personal Data Protection also provides for special categories of personal data, namely:

✓ ***personal data*** revealing racial or ethnic origin, political views, religious or philosophical beliefs or membership in trade union organizations, as well as genetic data, biometric data, data relating to health or data on the sex life or sexual orientation of the natural person;

✓ ***genetic data*** is personal data related to the genetic characteristics of the natural person that are inherited or acquired, revealing unique information about their physiology or health, and is particularly obtained by analyzing a biological sample of that natural person.

✓ ***biometric data*** is personal data obtained through specific technical processing of the physical and physiological characteristics of the natural person or characteristics of their behavior, enabling or confirming the unique identification of the natural person, and

✓ ***data related to health*** is personal data related to the physical or mental health of the natural person, including data on the received health care that reveal information about their health.

The processing of the special categories of personal data is prohibited, except when:

- the data subject has given explicit consent to the processing of the personal data for a single or more specific purposes;
- the processing is required for the purposes of performing the obligations and exercising the special rights of the controller or the data subject in the field of employment and social security and in social protection regulations, as allowed by law or collective agreement;
- the processing is necessary to protect the fundamental interests of the data subject or of another natural person;
- the processing is carried out within the permissible activities with appropriate safeguards by a certain foundation, association or any other non-profit organization with a political, philosophical, religious or trade union purpose and provided that the processing concerns only members of these organizations or their former members or persons who have regular contacts with them pertaining to their purposes and provided that the personal data is not disclosed outside that organization without the consent of the data subjects;
- the processing concerns personal data which has apparently been published publicly by the data subject;
- the processing is required for initiating, pursuing or defending legal claims or whenever the courts are acting within their jurisdiction;
- the processing is required for reasons of public interest based on law, proportionate to the purpose, while upholding the essence of the right to personal data protection, and providing adequate and specific safeguards for the fundamental rights and interests of the data subject;
- the processing is required for the purposes of preventive or occupational medicine, assessing employee work capacity, medical diagnosis, providing healthcare or social services or treatment or for the purposes of managing healthcare or social services and systems;

- the processing is required for the purposes of public interest in the field of public health and
- the processing is required for archiving in the public interest, scientific and historical research, or statistical purposes.

In April 2022, the Personal Data Protection Agency proposed new, additional amendments to the Law on Personal Data Protection, for the following reasons:

- the Law on Personal Data Protection has not fully implemented the solutions to ensure that the Agency has all the necessary resources for effectively executing its functions and powers, aiming to underscore its autonomy, independence and impartiality as provided for in 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, on the free movement of such data and on the repeal of Directive 95/46/EC (General Regulation on data protection). This situation was also noted in the 2021 Report on North Macedonia by the European Commission. These amendments are intended to establish complete autonomy and independence in the Agency's operations, ensuring it can function without influence (opinions and approvals) from other institutions while managing its resources (human and financial) and
- to align the mentioned Law with the novelties concerning the transfer of personal data being implemented in European Union member states (the Recommendations of the Board for personal data protection regarding European essential guarantees and the transfer measures), these amendments introduce new measures aimed at facilitating the work of controllers and processors in order to be able to transfer personal data to third countries and international organizations more easily.[17]
- The Law on Personal Data Protection and the corresponding by-laws in RNM govern personal data protection in a manner and to an extent consistent with full EU membership, without any delay in application. Therefore, unlike

17 Personal Data Protection Agency, 2022 Annual Report, p.10. Link: https://azlp.mk/wp-content/uploads/2023/.

other regulations harmonizing the national legislation with EU legislation, there are provisions with deferred application, that is, certain articles will be applied upon RNM's accession to the EU, while the legal framework for personal data protection is structured to automatically cease its validity upon RSM's accession to the EU, ensuring there is no duplication of regulations on the same issue, as it is already harmonized with EU standards within our country.

1.2 OTHER LAWS AND BY-LAWS IN THE FIELD OF PERSONAL DATA PROTECTION AND THE RIGHT TO PRIVACY

The widespread processing of personal data in the digital realm, coupled with rapid technological advancements and thus the potential for misuse, necessitates the revision of other laws that have an impact on privacy, personal data protection and the effective exercise of privacy rights in the online domain.

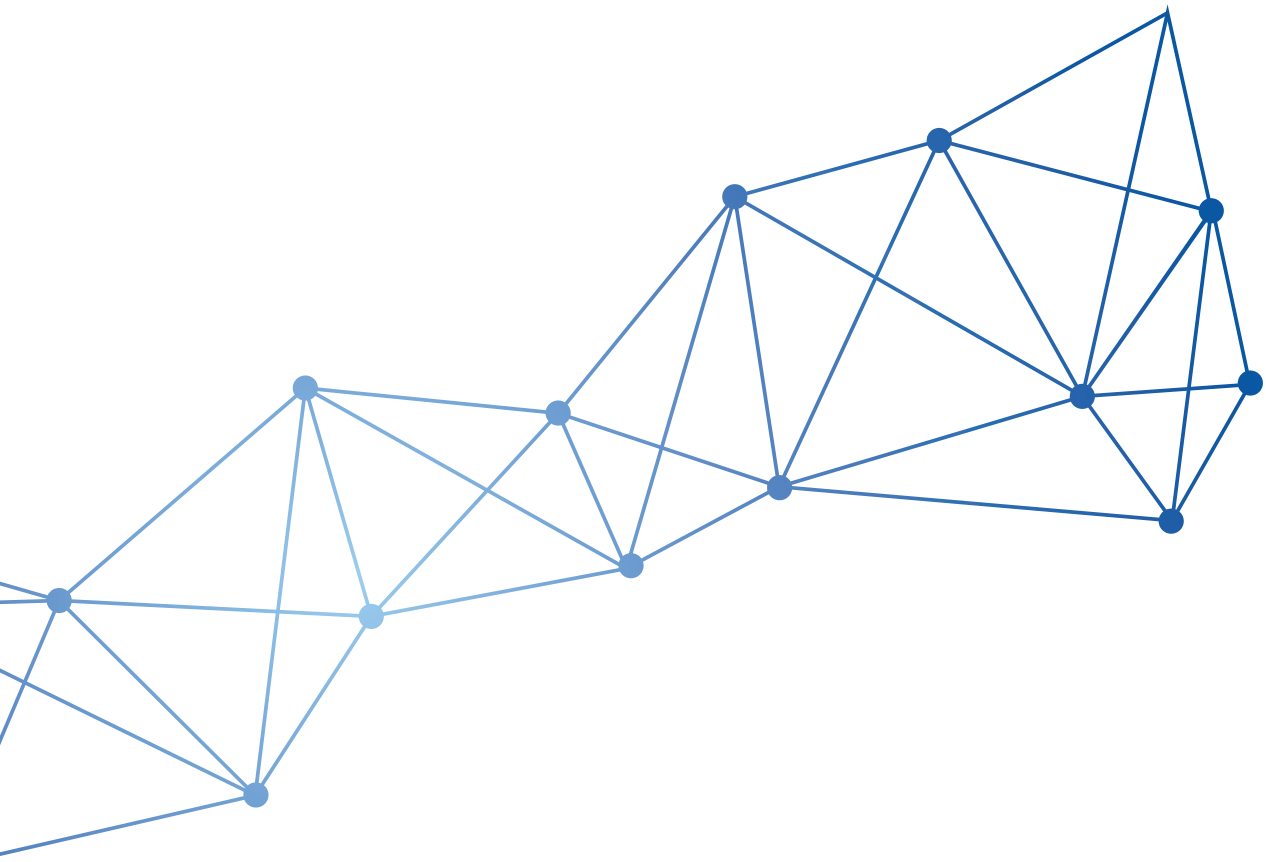


Table 1.
Other laws relevant for personal data protection

LAW	RELEVANT POSITIONS
Law on Payment Services and Payment Systems	Art. 126 "the payment service provider processes a payment service user's personal data in compliance with the LPDP,"; Art. 150 "the payment system operator performs personal data processing in compliance with the LPDP"
Law on the Prevention of Money Laundering and Financing of Terrorism	Art. 36; Art. 72(5); Art. 91(4) and Art. 182 "personal data may be used in accordance with the purposes prescribed by this law and in accordance with the regulations governing personal data protection"
Law on Healthcare	Art. 92-e "the personal data of PHI employees can be transmitted through an electronic communication network, provided that such data is safeguarded with suitable technical and organizational measures to ensure it remains unreadable during transmission"
Law on the Protection of Patients' Rights	Art. 25 "the patient has the right to confidentiality (secrecy) of their personal and medical data, which must be kept confidential even after the patient's death, in accordance with the law"
Law on Social Protection	Art. 24 "beneficiaries of social protection rights and services are assured confidentiality and the safe-guarding of their personal data, in in accordance with the law"
2021 Law on Census	Art. 3, 5, 8, 17, 25, 33, 39, 40. "authorized persons, as well as employees of the SSO, are obliged to keep all personal data confidential during and after the Census"

Law on Central Population Register	Art. 3 “the provisions of this law regulate the access and processing of personal data contained in the Register by other entities”
Law on Juvenile Justice	Art. 24 para. 6 - The register includes data obtained through notifications from the Ministry of Interior, the Public Prosecutor’s Office, the school or from another institution where the child receives care and education, as well as from their parents, i.e. guardians, the child, the victim and from another person. This information is treated confidentially in accordance with regulations pertaining to classified information and personal data protection.
Law of Civil Liability for Insult and Defamation	Article 8 of the ECHR - protection of private life, reputation and honor
Law on Criminal Procedure	Chapter XV Personal data protection
Law on the Protection of Whistleblowers	Entire law – a special mechanism to protect the whistleblower’s identity

In addition to the Law on the Ratification of the Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data[18], the Law on the Ratification of the Additional Protocol to the Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data, concerning the supervisory bodies and the cross-border data transfer[19] and the Law on the Ratification of the Protocol to Amend the Convention for the Protection of Individuals with regard to the Automatic Processing of

18 Official Gazette of RM – International Agreements, No. 7 of 1.02.2005.
19 Official Gazette of RM – International Agreements, No. 103 of 19.08.2008.

Personal Data20, the enhancement and safeguarding of privacy and personal data of the citizens of RNM is also regulated in other laws that regulate issues related to the storage, transfer and processing of personal data.

All laws and other regulations governing the collection, processing, storage, use and delivery of personal data must be in compliance with the Law on Personal Data Protection. It envisages the adoption of by-laws – rulebooks, registers, lists, etc., to provide more detailed regulation of specific issues within this domain. The responsible authority for adopting these by-laws is the Director of the Personal Data Protection Agency, within a legally defined timeframe of 18 months following the law's enactment (24.02.2020). The table below shows that most of the by-laws were adopted in May 2020, and amended two years later, in August 2022.

Table 2.
By-laws relevant for personal data protection

1.	Rulebook on data processing security ("Official Gazette of the Republic of North Macedonia" no. 122/20)
2.	Rulebook on the content and form of the act for performance of video surveillance ("Official Gazette of the Republic of North Macedonia" no. 122/20)
3.	Rulebook for amending the Rulebook on the content and form of the act on the way video surveillance is performed ("Official Gazette of the Republic of North Macedonia" no. 280/21)
4.	Rulebook on the content of the analysis of the goal, i.e. the goals for which the video surveillance is set up and the report of the periodic evaluation of the results achieved by the video surveillance system ("Official Gazette of the Republic of North Macedonia" no. 122/20)
5.	Rulebook on the method for supervision performance ("Official Gazette of the Republic of North Macedonia" no. 122/20)
6.	Rulebook on data transfer ("Official Gazette of the Republic of North Macedonia" no. 122/20)

20 Official Gazette of RNM – International Agreements, No. 152 of 7.7.2021.

7.	Rulebook on personal data protection training ("Official Gazette of the Republic of North Macedonia" no. 122/20)
8.	Rulebook on the form and content of official identification card and the method for issuance and withdrawal ("Official Gazette of the Republic of North Macedonia" no. 122/20)
9.	Rulebook on the process for data protection impact assessment ("Official Gazette of the Republic of North Macedonia" no. 122/20)
10.	Rulebook on the form and content of the request for determining violation of provisions under the law on personal data protection ("Official Gazette of the Republic of North Macedonia" no. 122/20)
11.	Rulebook on the method of reporting personal data breach ("Official Gazette of the Republic of North Macedonia" no. 122/20)
12.	List of processing operation types that require data protection impact assessment ("Official Gazette of the Republic of North Macedonia" no. 122/20)
13.	List of processing operation types that do not require data processing impact assessment ("Official Gazette of the Republic of North Macedonia" no. 122/20)
14.	Decision on establishing standard contractual clauses for transfer of personal data to third countries* ("Official Gazette of the Republic of North Macedonia" no. 280/21
15.	Decision on establishing standard contractual clauses between controllers and processors* ("Official Gazette of the Republic of North Macedonia" no. 280/21)
16.	Decision on determining the Methodology for the harmonization of the sectoral legislation ("Official Gazette of the Republic of North Macedonia" no. 38/22)
17.	Rulebook to complement the Rulebook on the content of the analysis of the goal, that is, the goals for which the video surveillance is set and the report of the periodic evaluation of the results achieved by the video surveillance system ("Official Gazette of the Republic of North Macedonia" no. 183/22).

18	Rulebook to complement the Rulebook on the form and content of the request for determining a violation of the provisions of the law on the protection of personal data ("Official Gazette of the Republic of North Macedonia" no. 183/22).
19.	Rulebook to complement the Rulebook on the Method of Reporting Violation of Personal Data Security ("Official Gazette of the Republic of North Macedonia" No. 183/22).

1.3 Strategic documents

1.3.1 STRATEGY FOR EXERCISING THE RIGHT TO PERSONAL DATA PROTECTION 2018-2022

This strategic document was prepared with the support of an international expert addressing the global trends in personal data protection. Throughout its development, attention was paid to the pervasive networked society, the rapid dissemination of information via the Internet, the extensive data analysis, the concepts of e-government with interconnected databases, but also the increasing international data flow, the issues of national and global security and the increased public demands for accountability and transparency accompanied by heightened oversight by supervisory authorities.[21] A significant innovation embedded within this strategic document lies in its commitment to educating children on the importance of personal data protection.

The annual report of the PDPA, specifically within the section detailing the Agency's strategic objectives for the period spanning 2018 to 2022 emphasizes:

- Republic of North Macedonia to be recognized as a country providing an adequate level of personal data protection;
- Establishing a self-sustaining system for personal data protection;
- Continual increase of public awareness and culture regarding personal data protection;
- Ongoing enhancement of compliance among controllers and processors of personal data;
- Continual cooperation with partners;
- Enhanced efficiency of administrative procedures;
- Effective management of international matters; and
- Well-trained and motivated team prepared to confront challenges.[22]

Nevertheless, by the end+ of 2022, the Agency secured approval for a series

21 Akademik: The new Strategy for the implementation of the right to personal data protection, published: 4.12.2017. Available at: https://akademik.mk/novata-strategija-za-sproveduvane-na-pravoto-za-zashtita-na-lichnite-podatotsi/.
22 Personal Data Protection Agency, 2022 Annual Report, p.6. Link: https://azlp.mk/wp-content/uploads/2023/.

of events aimed at commencing the development of a new ten-year Strategy dedicated to upholding the right to personal data protection, with the support of the TAIEX program of the European Union , which should be adopted in due time.

1.3.2. COMMUNICATION STRATEGY 2018-2023

In its most recent report[23], the Agency highlights the implementation of activities outlined in the Communication Strategy (2018-2023), encompassing:

- Education and information exchange through direct meetings with journalists/media and organization of trainings
- Education and awareness-raising by drafting informative and educational materials focused on key aspects of personal data protection tailored to the target groups: children, minors, adolescents
- Sharing concise updates on case outcomes and actions taken through regular announcements on the Agency's website
- Organizing joint events or meetings dedicated to the topic of personal data protection through the involvement of various institutions
- Promoting and educating about personal data protection on social media platforms by highlighting good practices and conducting analyses of bad practices in sharing personal data, and
- Continuous active participation in international forums and events, participation in mechanisms for exchange of experiences, implementing models and best practices.

23 Personal Data Protection Agency, 2022 Annual Report, p.31. Link: https://azlp.mk/wp-content/uploads/2023/.

II.
INSTITUTIONAL FRAMEWORK

2. Institutional framework

2.1. PERSONAL DATA PROTECTION AGENCY

2.1.1 RIGHTS AND COMPETENCIES

The Agency operates as an autonomous and independent state authority, entrusted with the oversight of the lawfulness of personal data processing activities within the territory of the Republic of North Macedonia, as well as the protection of the fundamental rights and freedoms of natural persons in relation to the processing of their personal data. The Agency maintains complete autonomy in political, financial, and functional matters while executing its duties, and is responsible for formulating policies, measures, and actions aimed at ensuring the consistent enforcement of national-level personal data protection regulations.

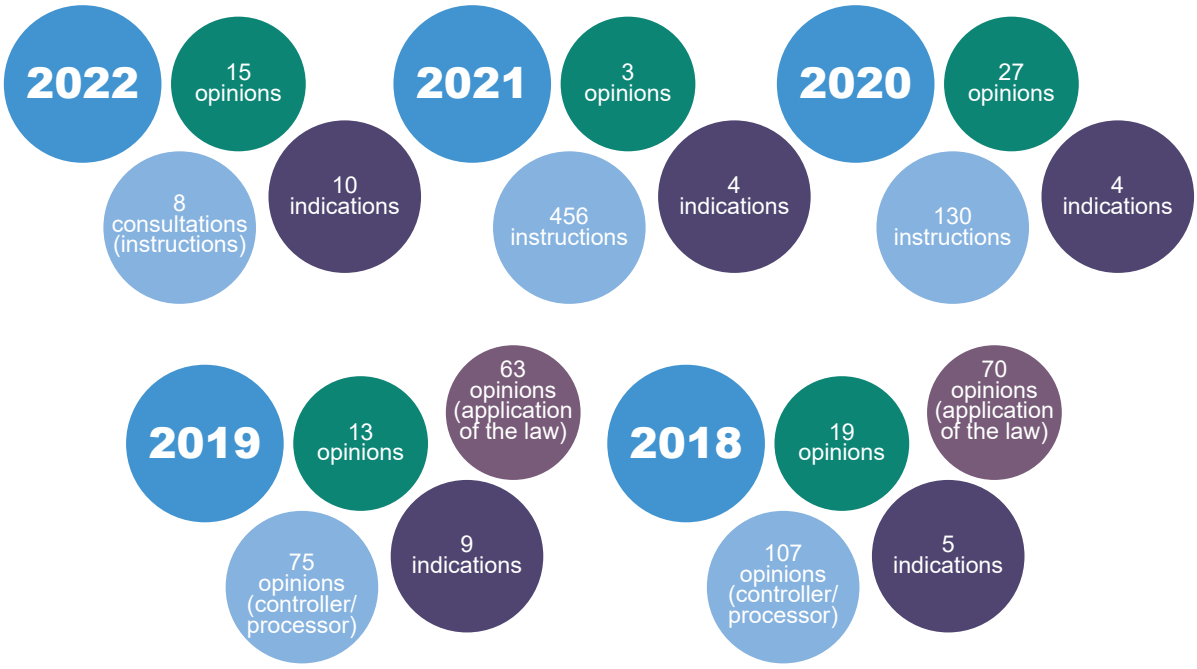
Competencies, tasks and powers of the Agency
The Agency shall not be competent to supervise processing operations of courts acting in their judicial capacity, with the exception for supervision of lawfulness of actions taken during other personal data processing actions done by the courts, in accordance with the law.
Article 64, paragraph 2 LPDP

The responsibility for ensuring the conformity of all (secondary) laws and regulations with the provisions outlined in the Law on Personal Data Protection lies within the jurisdiction of the Personal Data Protection Agency. Furthermore, the Agency is obligated to align the legal framework of the Republic of North Macedonia with the legislation of the European Union and the legal instruments of the Council of Europe in this realm. To facilitate this process, the Agency has initiated to adopt a Decision outlining the Methodology for the Harmonization of Sectoral Legislation[24]. This methodology provides clear guidelines that govern the actions of ministries during the harmonization process. This encompasses the evaluation of existing laws and conducting assessments of their impact from a personal data protection perspective. In other words, ministries are

24 Decision outlining the Methodology for the Harmonization of Sectoral Legislation, Official Gazette of the Republic of North Macedonia, no. 38/22.

mandated to ensure that their legislation, particularly those concerning privacy and personal data protection, aligns with the LPDP.

The Agency proactively ***issues opinions***[25] or responds to requests from entities such as the Parliament, the Government, and other institutions and bodies. These opinions encompass legislative and administrative measures designed to safeguard the rights and freedoms of natural persons concerning the processing of personal data. In essence, the Agency provides opinions on proposed regulations within the realm of personal data protection. Furthermore, authorities have the option to seek consultation with the Agency. Lastly, the Agency may also provide indications when state authorities tasked with defining matters related to the processing and protection of personal data should stipulate them in laws, by-laws or other regulations.



Source: Personal Data Protection Agency, Annual Reports 2022-2019

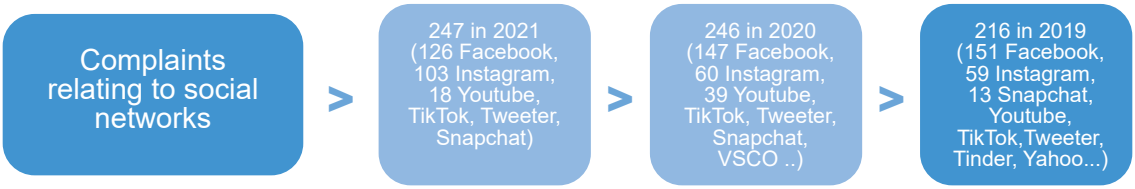
25 Annex I provides a list of draft laws, by-laws and other materials for which an opinion has been provided in 2022.

Until the adoption of LPDP in 2020, little progress was observed in the process of harmonizing the sectoral legislation with the Law on Personal Data Protection. For example, certain opinions and recommendations provided by the Agency (formerly known as the Directorate), such as the Law Amending the Law on Vehicles, the Law Amending the Law on Banks, and the Law on Prevention of Money Laundering and Financing of Terrorism, were not duly adhered to, which is documented in the Annual Report of the Agency.[26] The enactment of the LPDP marked the start of the gradual process of rectifying the previous unfavorable trend of non-consolidation and non-compliance, specifically regarding the non-submission of legislative proposals for laws and by-laws, and this paved the way for greater consistency within the legal framework of the Republic of North Macedonia, ensuring more consistent adherence to the principles governing personal data protection.

Pursuant to Article 70 of the LPDP, the Agency prepares an annual report on its work, which may include a list of violations for which it was notified, as well as the types of measures taken. The latest report[27] noted that 300 complaints were acted upon last year. Out of these cases, 77% pertain to violations involving social networks, while the remaining 23% concern other types of complaints within the realm of personal data protection. These encompass the failure to provide the conditions for exercising data subjects' rights, particularly the rights of access, rectification, or erasure of personal data, the processing of personal data through video surveillance systems and instances of failing to provide adequate prior notification to data subjects regarding the collection, processing, and storage of their personal data fall within this category[28].

26 Personal Data Protection Directorate, 2018 Annual Report, p.12. Link: https://azlp.mk/wp-content/uploads/2022/12/godisen_izvestaj_dzlp_2018.pdf.
27 Personal Data Protection Agency, 2022 Annual Report. Link: https://azlp.mk/wp-content/uploads/2023/.
28 Personal Data Protection Agency, 2022 Annual Report, p.18. Link: https://azlp.mk/wp-content/uploads/2023/.

This analysis underscores the significance of the large number of 232 reported complaints linked to social networks in the year 2022. Among the reasons cited for these complaints, the most notable categories involve complaints from natural persons. These encompass issues such as the presence of fake profiles, unauthorized access to personal profiles (hacking), the dissemination of third-party photos, videos, and audio recordings on third-party social media profiles, as well as complaints related to internet-based insult, defamation, and blackmail. When categorizing these complaints by the specific social network implicated, the majority are related to Facebook (116), then Instagram (103), and a subset of complaints (18) is linked to YouTube, TikTok, Twitter, Snapchat, etc.[29]



An interesting trend emerges since 2019 onwards. During this period, there has been a notable uptick in citizen complaints concerning the proliferation of fake profiles on social networks, as well as reports involving criminal activities, insults, blackmail, and threats. However, the Agency lacks the jurisdiction to take action on these matters.

29 Personal Data Protection Agency, 2022 Annual Report, p.18. Link: https://azlp.mk/wp-content/uploads/2023/.

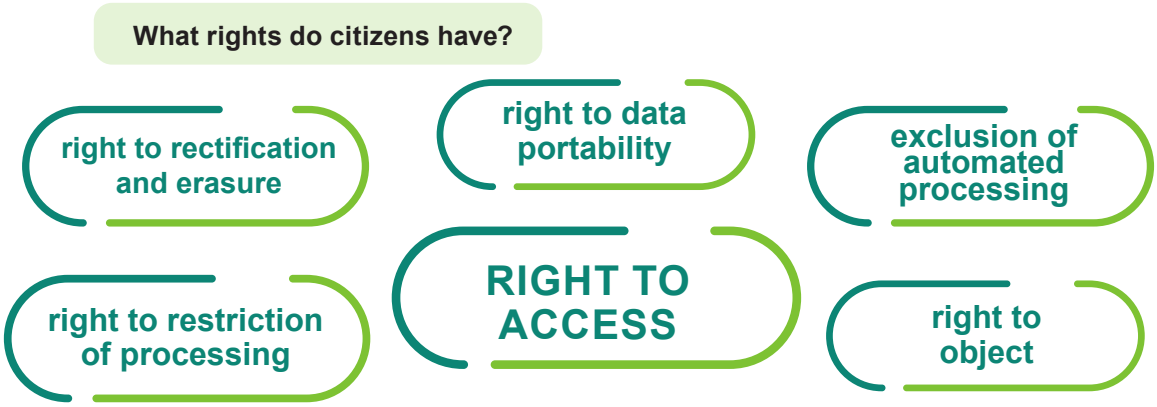
III.
CITIZEN RIGHTS AS DATA SUBJECTS

3.Citizen rights as data subjects

Every citizen should be aware that the processing of their personal data is conducted in a manner and in a form established by law. Any natural or legal person, a public administration body, state authority, etc., is obligated to take all essential measures to present the information outlined in the LPDP in a clear, transparent, easily understandable, and readily accessible format. In other words, it must be done using clear and simple language especially when disseminating information intended for children.

THE DATA SUBJECT IS ENTITLED:

- to be informed about the identity of the data controller and their representative in the Republic of Macedonia
- to know which personal data is stored for them in electronic or paper form
- to know the purposes of the processing of their personal data
- to conduct an inquiry into the filing system
- to know the users or categories of data users
- to access and rectification of data
- to disagree with the use of the data for commercial purposes or its transfer to third parties for such purposes



Every citizen holds the right to ***request access*** to their personal data held by natural or legal persons acting as data controllers. It is a legal obligation on the part of the data controller to inform the citizen about the nature and categories of personal data they possess, their data processing methods, method and sources of data collection, conditions for data sharing, data retention durations, and the presence of any automated decision-making processes, including profiling. Furthermore, should the individual whose data is being processed suspect inaccuracies or incompleteness in their data, or believe that additional information is necessary to fulfill the intended purpose of data processing, they are entitled to ***request the rectification and supplementation*** of their personal data. Conversely, in situations where an individual deems their personal data to be no longer necessary for the originally intended purpose, they have the right to request the exercise of their ***right to deletion***. This right can also be invoked when the individual no longer consents to the data processing, has objected to the personal data processing, believes that the data has been unlawfully processed, or was a minor or remains a minor at the time of data collection. ***The right to restrict data processing*** can be invoked when the individual disputes the accuracy of their personal data, perceives the processing as unlawful, deems the data unnecessary for the controller's purposes, and requires confirmation that the controller's legitimate interests outweigh the individual's interests as a data subject. Moreover, if the individual believes that their personal data is being processed for public or legitimate interests, including profiling, for the purposes of direct marketing and associated profiling, or for scientific, statistical, historical purposes and

research, they have the option to ***object*** to the processing of their personal data. Individuals have ***the right to opt out of automated decision-making and profiling*** that may lead to legal consequences or significantly impact them. Additionally, every citizen possesses the legal right to receive their personal data in a structured, commonly used, or machine-readable format. Simultaneously, individuals can request the transfer of this data to another data controller. This right to data portability applies specifically to personal data processed based on consent or contractual agreements and through automated means.

3.1 What happens when there is a personal data security breach?

The Law on Personal Data Protection meticulously regulates breaches of personal data security. In such instances, the data controller is obligated to promptly inform the Agency about the breach of personal data security, without delay and within a maximum of 72 hours from the moment they become aware of it. There is an exception to this rule if the breach of personal data security poses a risk to the rights and freedoms of natural persons. In cases where notification to the Agency is not submitted within the 72-hour timeframe, an explanation for the delay must accompany the notification[30]. Furthermore, the data processor is also obligated to immediately notify the data controller upon becoming aware of a personal data security breach. The data controller is responsible for documenting all instances of personal data security breaches, including facts about the personal data security breach, its consequences, and the remedial actions taken (Art. 37 LPDP).

30 The notification shall, at least: (a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of filing systems concerned; (b) communicate the first and last name, and contact details of the data protection officer or other contact point where more information can be obtained; (c) describe the likely consequences of the personal data breach; (d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects. Art.37 para.3 of the LPDP.

Personal data security breach
In the event of a breach of personal data security, the operator of public electronic communication services is legally obliged to take prompt action. Within 24 hours from the moment of discovering the breach, they must submit a notification of the personal data security breach to the Personal Data Protection Agency.
Within the same timeframe, they are obligated to notify the affected subscriber or natural person.
Article 167, Law on Electronic Communications

If a personal data security breach is likely to pose a significant risk to the rights and freedoms of natural persos, the data controller is obliged to promptly inform the data subjects about the spersonal data security breach. This notification31 to the data subject should provide clear and straightforward explanations regarding the nature of the personal data security breach. If the data controller fails to inform the data subject about the personal data security breach, and the Agency determines that there is a probability of a high-risk breach, the Agency may require the controller to provide such notification or decide that one of the legal requirements has been met (Art. 38 LPDP).

In essence, if an individual believes that their legally protected rights have been violated, they may submit a request to the Agency for determining a violation of the provisions outlined in the Law on Personal Data Protection, through a special form[32]. In the form, the person whose rights have been violated must state the reasons and data about the controller that they believe has violated their statutory rights. Subsequently, the Agency, within the legally specified deadline, and through a decision, informs the petitioner about the course and outcome of the procedure, and informs them about the possibility of seeking judicial protection. Every data subject holds the right to seek effective judicial protection if the Agency fails to act on their request or does

31 The notification to the data subject shall not be required if any of the following conditions are met: (a) the controller has implemented appropriate technical and organizational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorized to access it, such as the encryption; (b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph (1) of this Article is no longer likely to materialize; (c) if the notification would require disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner. Art.38 para.3 of the LPDP.
32 The form is provided in Annex II.

not inform the data subject of the procedure's outcome within three months of submitting the request. In any case, on the submitted request, the Agency performs supervision in accordance with the established legal procedure (Art.97 and 98).

3.2. Requests to the Agency for determining violations of the Law on Personal Data Protection

Statistically, in the year 2022, there was an uptick in notifications from public sector data controllers, as compared to the preceding year, 2021. This surge in notifications can be construed as a positive development, signifying an enhanced awareness of and correct application of the LPDP. Hence, in 2022, the public sector reported a total of 5 incidents involving breaches of personal data security, a substantial increase from the single incident reported in 2021. Conversely, private sector data controllers accounted for the remaining 14 out of the 19 notifications received in 2022. In contrast, 2021 saw a total of 9 notifications, with 8 originating from private sector controllers. Despite the mounting number of reported breaches of personal data security, data controllers continue to grapple with the challenge of distinguishing between mere incidents and genuine violations of legally safeguarded rights. Furthermore, they struggle to differentiate between probable risks to the controller and probable risks to the rights and freedoms of the data subjects involved. According to the PDPA[33], data controllers have not yet fully established a system for documenting and reporting such incidents. Consequently, they are hesitant to report personal data security breaches to the Agency, even though they are legally obligated to do so.

These concerns are underscored by the findings of a recent special oversight conducted by the Agency within the Office for Management of Registers (OMR), which followed a case involving the misuse of personal data belonging to Macedonian citizens. This case centered on serious deficiencies in the

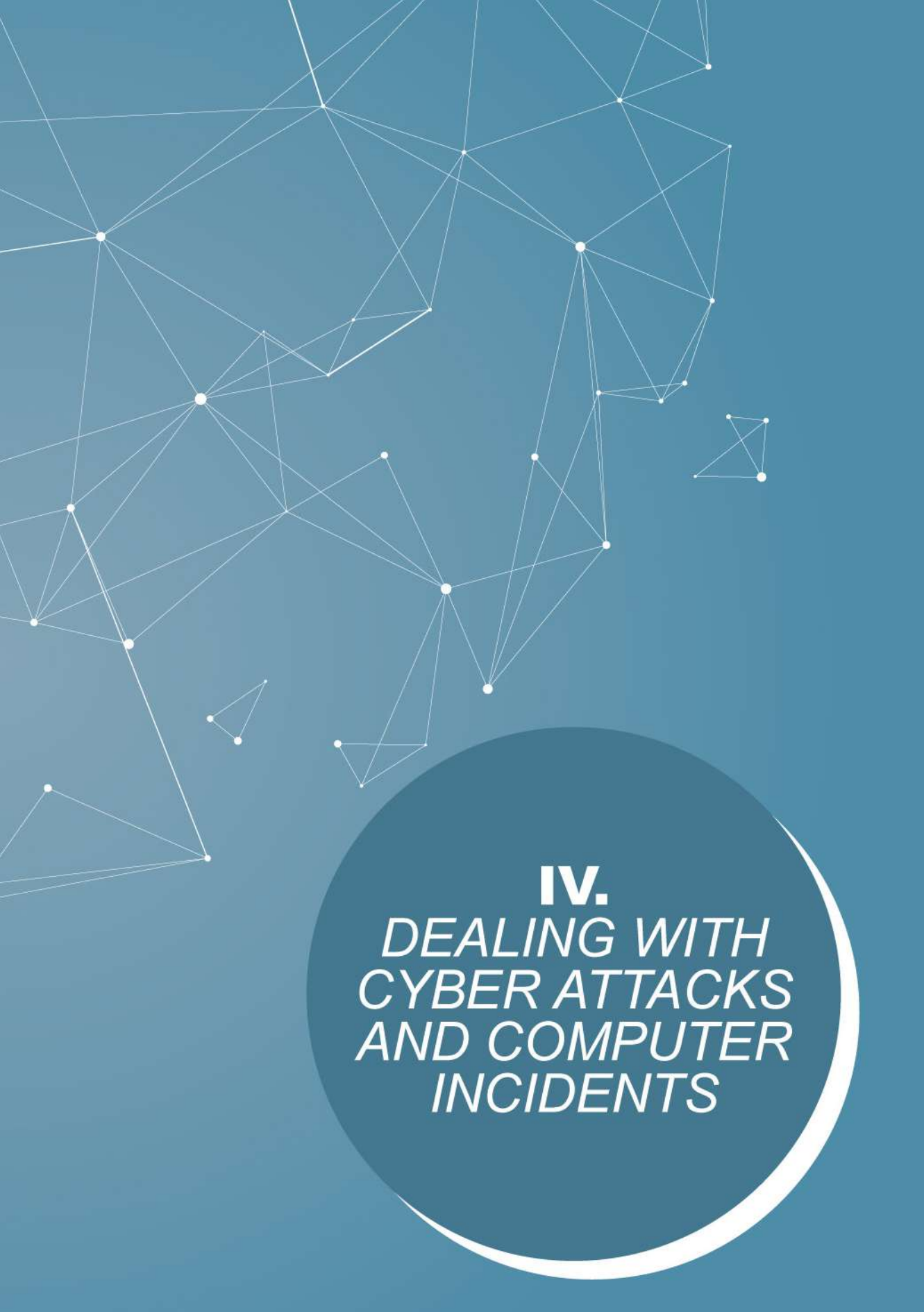
33 Personal Data Protection Agency, 2022 Annual Report, p.14. Link: https://azlp.mk/wp-content/uploads/2023/.

digitalization of registers. Specifically, in July 2023, the State Commission for the Prevention of Corruption (SCPC) unveiled a case related to a contentious tender awarded to a private company for digitizing registers containing information on births, deaths, and marriages of citizens of RNM[34].

In alignment with recurring observations in annual reports, the primary issue identified was the absence of an adequate system for documenting and reporting incidents. In this particular instance, the PDPA noted that "The responsible data controller, i.e. OMR, lacked records pertaining to the hardware, servers, and software applications involved in processing personal data. Furthermore, there were no entry logs in the register, personal data was stored on a server without access tracking, and economic operators had collected data without the supervision of OMR officials. The room where personal records were scanned lacked physical security, and there was no way to determine who accessed the software modules containing scanned records and personal data. Transfer media were not protected, and there was no proof of prevention of unauthorized access to personal data, leaving unanswered questions about who accessed the data, where it was taken, where it ultimately ended up, and for what purposes[35]."

The Personal Data Protection Agency was requested to perform a special oversight at OMR, in order to ascertain who had access to the scanned personal data documents, how they were stored, whether they were protected, whether the established system for their protection was effective and efficient and whether there had been illicit utilization of this data.

34 Meta.MK: Concerns regarding compromised registry books and the illicit trade of individuals' personal data, published on 19.07.2023, source available at: https://meta.mk/matichnite-knigi-probieni-trgovija-so-lichnite-podatoci-na-gragjanite/.
35 Meta.MK: Concerns regarding compromised registry books and the illicit trade of individuals' personal data, published on 19.07.2023, source available at: https://meta.mk/matichnite-knigi-probieni-trgovija-so-lichnite-podatoci-na-gragjanite/.



IV.
DEALING WITH CYBER ATTACKS AND COMPUTER INCIDENTS

4. Dealing with cyber attacks and computer incidents

Expanding upon the previous case, it is important to emphasize that in safeguarding personal data against cyberattacks or computer incidents, individuals whose personal data is compromised are not engaged in an "institutional battle" to protect their data because in such cases, the target is not the individual as a data subject but rather the data controller. Notably, controllers holding substantial volumes of personal data, such as state institutions, banks, telecom operators, airlines, hospitals, etc., are prime targets for cyberattacks, often leading to extortion attempts aimed at selling back the compromised or hacked data. Consequently, the onus for protection and recovery largely falls on the data controller rather than on the individual, with the individual often unaware, albeit unlawfully, of the fate of their data.

Hence, MKD-CIRT has been incorporated into the institutional framework for personal data protection. The National Computer Incident Response Center (MKD-CIRT),[36] serves as the official national point of contact and coordination for addressing security incidents within networks and information systems. It identifies and responds to security incidents and risks, operating within the Agency for Electronic Communications. MKD-CIRT's constituents include:

- All ministries, public administration, and government services in the Republic of Macedonia.
- Operators of critical infrastructure within the Republic of Macedonia, and
- Large organizations in sectors such as banking, transportation, communication, healthcare, energy, and other strategic sectors in the Republic of Macedonia.

MKD-CIRT offers a reporting mechanism for computer incidents on its website. The institution plays a preventive role, employs methods to intercept computer attacks and incidents, maintains international partnerships with similar entities, and ensures rapid information flow and threat notification.

36 MKD-CIRT, https://mkd-cirt.mk/za-nas/

In practice, a significant issue arises from the fact that a substantial portion of the entities mentioned above, which could and should be engaged, are largely unaware of these opportunities. Consequently, this underscores the need for increasing awareness and fostering a culture of cyber attack prevention and swift incident response as an effective mechanism for safeguarding personal data.

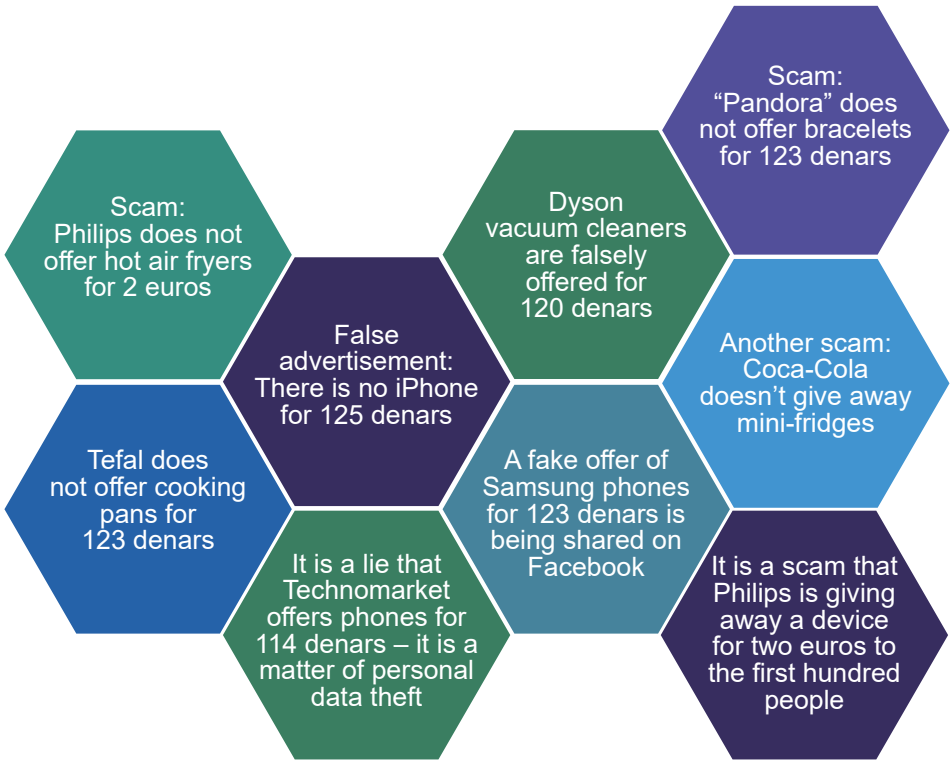
4.1 Examples of computer attacks leading to potential misuse of personal data

1. The Macedonian public was shaken by the revelation[37] that user data, including citizens' personal information, had been stolen from the Health Insurance Fund. Widespread panic ensued following statements from the Prime Minister and the Minister of the Interior, indicating that the Fund's information system had fallen victim to a "ransomware" attack, and hackers demanded a ransom for the system's release[38]. To expedite resolution, operational teams from the Ministry of Health and the HIF collaborated with experts from Germany and other international partners[39].

2. However, amidst frequent hacker attacks on state institutions, schools, and shopping centers, part of broader hybrid warfare, within RNM and beyond, Macedonian citizens face daily fraudulent activities on social networks. It appears that the country is a vulnerable target for various scams, with citizens often recklessly sharing personal information in pursuit of "cash prizes," "trips," and "free products." In 2023[40] alone, over 20 fraud and misuse of

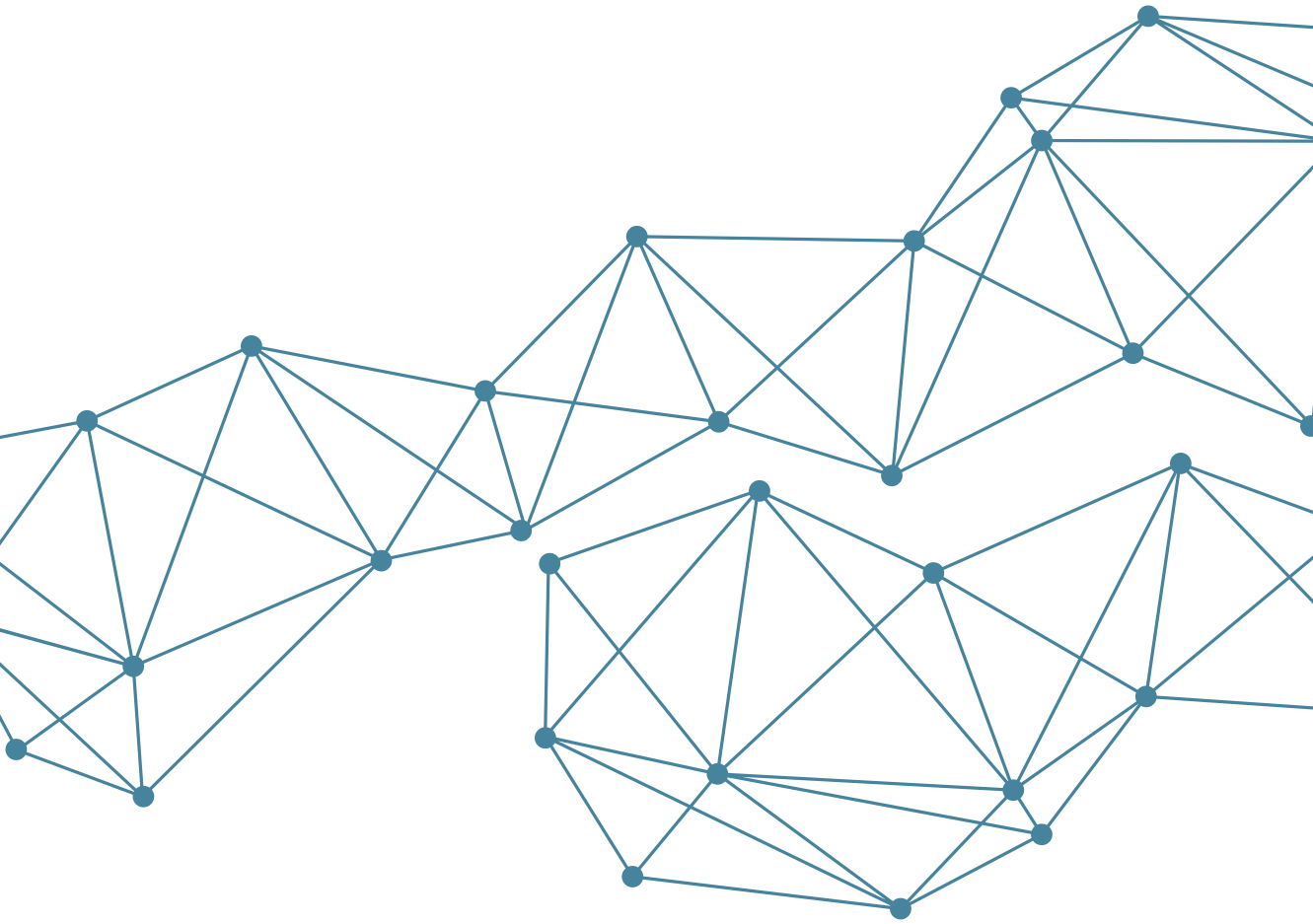
37 eMagazin: The Health Fund asserts that citizens' data remains secure and has not been subject to theft, published on 17.02.2023, available at: https://emagazin.mk/od-fondot-za-zdravstvo-tvrdat-deka-podatocite-na-gra-anite-se-bez-bedni-i-deka-ne-se-ukradeni/.
38 eMagazin: HIF's system hacked with "ransomware", hackers demand a ransom to "free" it, published on 17.02.2023, available at: https://emagazin.mk/sistemot-na-fzo-hakiran-so-virusot-ransomware-hakerite-baraat-otkup-za-da-go-oslo-bodat/.
39 eMagazin: Foreign experts will be tasked with repairing the Health Insurance Fund system following the hacker attack, published on 16.02.2023, available at: https://emagazin.mk/stranci-e-go-opravuvaat-sistemot-na-fondot-za-zdravstveno-osiguruva-e-po-hakerskiot-napad/.
40 Source Meta.mk, News agency, link: https://meta.mk/tag/lichni-podatotsi/.

personal data attempts occurred through specially created Facebook pages with similar content. Uninformed citizens readily share their credit or debit card details, only to have them quickly exploited, without getting the promised "rewards."



3. A hacker attack on the website of the State Election Commission on the Election Day, as well as the accusations of technical weaknesses of the application, raised concerns about institutional safeguards for the electoral process.The primary source for monitoring election results, the Commission's website, can be inaccessible. Journalists and the public were left without information from the SEC for hours.

Although the SEC is subscribed to implement protective measures designed to swiftly thwart such attacks and restore the server of the hacked site, international telecommunications company A1 Austria had to intervene to halt the attack[41].



41 Source IRL, investigative reporting laboratory, link://irl.mk/khibridni-voni-ko-dozvoli-da-se-khakne-izborniot-den/

V.

COMPETENCES OF THE JUDICIARY AND THE PUBLIC PROSECUTION IN ENABLING EFFICIENT JUSTICE FOR PERSONAL DATA PROTECTION AND THE RIGHT TO PRIVACY IN THE DIGITAL SPACE

5. Competences of the judiciary and the public prosecution in enabling efficient justice for personal data protection and the right to privacy in the digital space

Every citizen of RNM, as a data subject, possesses the right to effective judicial protection if they believe their rights have been violated due to improper processing of their personal data in contravention of the LPDP. Furthermore, every individual has the right to effective judicial protection against legally binding decisions issued by the Agency that pertain to them, without the need to exhaust alternative administrative or extrajudicial means of legal recourse.

Authorizations
The Agency possesses the authority to report violations of the provisions outlined in this law to the courts, as well as, as necessary, to initiate or participate in legal proceedings aimed at enforcing the provisions of this law.
Art. 66 par.5, LPDP

Data subjects exercise their rights by filing a lawsuit with the competent court, in accordance with the law.

Conversely, the Public Prosecutor's Office, in the spirit of adhering to the LPDP, fully incorporates the right to personal data protection. Within the Republic of North Macedonia, the Public Prosecutor's Offices, including the Public Prosecutor's Office of the Republic of North Macedonia, higher public prosecutor's offices, and basic public prosecutor's offices, conduct the collection, storage, and processing of personal data within their respective areas of responsibility for the purpose of prosecuting the perpetrators of crimes and misdemeanors. To facilitate criminal legal proceedings in specific cases, public prosecutor's offices process all data necessary for the criminal legal process. This personal data processing occurs both in paper form and electronically, and if necessary and in accordance with the law, personal data may be exchanged with other institutions to fulfill legal obligations and serve the interests of processing in criminal legal proceedings.

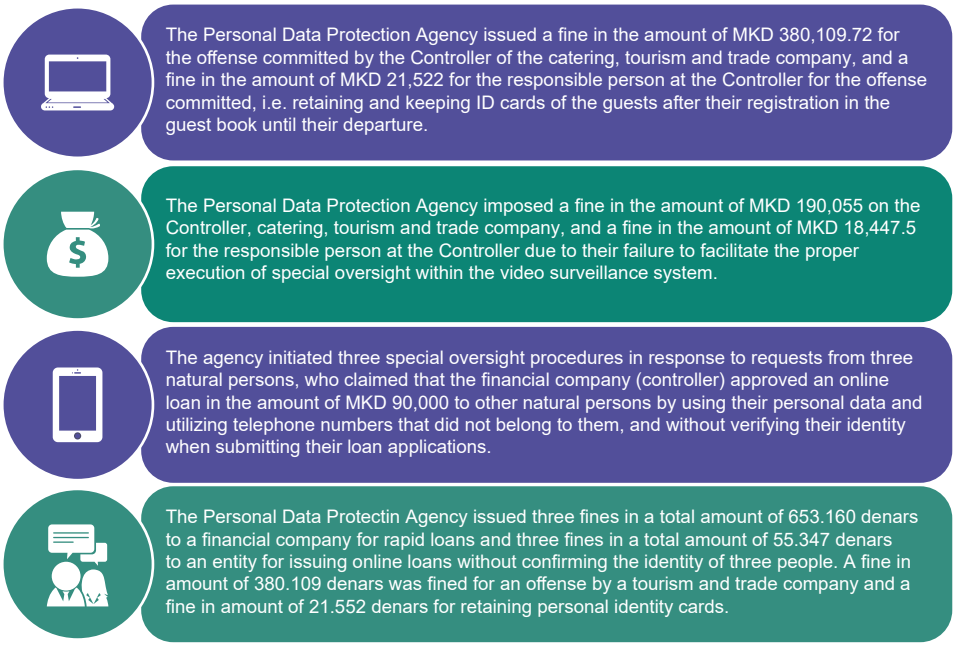
5.1. Case law in the realm of personal data protection and the right to privacy

5.1.1 JUDICIARY

Every individual, in addition to the right to submit requests to the Agency, holds the right to effective judicial protection against decisions rendered by the Agency. Additionally, individuals have the right to seek effective judicial protection against controllers or processors. Controllers, conversely, have the option to file a lawsuit with the Administrative Court, i.e. to initiate administrative disputes should they disagree with decisions made by the Personal Data Protection Agency.

In the years 2018 and 2019, a total of 25 administrative disputes were initiated. Among them, administrative courts issued decisions (judgements and decisions), with 23 cases confirming the Agency's decisions. This serves as a testament to the Agency's competence in consistently applying the Law on Personal Data Protection. In 2020, 10 new administrative disputes arose concerning decisions made by the Agency, while 19 judgments were issued for disputes initiated in previous years. In 2021, 20 administrative disputes were initiated against the Agency's decisions, leading to the preparation of 20 responses to lawsuits submitted to the Administrative Court. In the current year, 18 decisions were received from administrative courts. In 2022, 7 administrative disputes were initiated against the Agency's decisions, leading to the preparation of 7 responses to lawsuits submitted to the Administrative Court. During the analyzed year, the Administrative Court issued 10 decisions in connection with initiated administrative disputes.

Furthermore, should citizens of the Republic of North Macedonia suffer material or non-material damages due to violations of the LPDP's provisions, they possess the right to seek compensation from the controller or processor for the harm endured.



Regarding criminal and legal protection, the Criminal Code stipulates that a person who, against the conditions established by law, collects, processes, or utilizes personal data without the consent of the data subject may face a fine or imprisonment of up to one year. Likewise, the same penalties are prescribed for an offender who unlawfully breaches a computer information system containing personal data with the intent to benefit themselves or another or to cause harm to others.

The low penalties associated with the misuse of personal data and violations of the right to privacy, including in the digital realm, naturally lead to penalties that tend to lean towards the legally mandated minimum or suspended sentences.

An examination of sentences imposed over the past three years reveals that judges often impose fines amounting to 30 daily fines, equivalent to MKD 18,450. In certain cases, they opt for a higher penalty of 50 daily fines, or MKD 30,750. Additionally, suspended sentences of three months in prison are rendered in other instances, which do not take effect if the perpetrator refrains from committing new offenses during the probationary period, typically set at one year by judges.

For a tabular presentation of randomly selected judgments from the Basic Courts in RNM, spanning from 30.12.2019 – 1.08.2023, 2023, along with their legal basis and offense explanations, please refer to Annex IV.

5.1.2. PUBLIC PROSECUTOR'S OFFICE

Among the significant cases handled by the public prosecutor's offices in RNM concerning the protection of privacy and personal data are those related to the "Public Room" groups established on the "Telegram" social network.

In the case widely known as "Public Room 1," the Basic Public Prosecutor's Office in Skopje issued an Order on 05.02.2021, to initiate an investigative procedure against two individuals for the crime of producing and distributing child pornography, as per Article 193a, paragraph 3, in conjunction with paragraph 1 of the Criminal Code. Between 19.12.2019, and 28.01.2020, the two suspects, who served as the founders and moderators of the group, were tasked with overseeing the textual and audio-visual content shared by group members. However, they intentionally permitted the dissemination of content within the group, including audio-visual material depicting explicit exual acts involving a child. The "Public Room 1" group on the "Telegram" social network was subsequently shut down. Both the creator and administrator of the groups were each sentenced to 4 years in prison.

Regarding the case publicly known as "Public Room 2," it is currently in the preliminary investigation phase. On 27.1.2021, the Basic Public Prosecutor's Office in Skopje, through the Ministry of Interior, sought real user profile data from the international service provider, Telegram, about the creators, administrators, and members of the group. Several public prosecutor's offices throughout the country are concurrently involved in establishing criminal liability within the "Public Room 2" group. Orders for expert opinions and requests for data provision have been issued as follows:

- The Basic Public Prosecutor‘s Office in Veles opened a case and issued an Order to initiate an investigative procedure against an individual regarding “Public Room 2” due to well-founded suspicions of committing the crime of producing and distributing child pornography under Article 193-a, paragraph 3, in conjunction with paragraph 2. Notably, video recordings featuring child pornography were discovered during the examination of the suspect’s mobile phone.
- The Basic Public Prosecutor‘s Office in Bitola opened a case linked to “Public Room 2.” The office issued orders for the examination of a CD and a mobile phone to gather material evidence and ascertain facts in the case. A decision on the subsequent course of the procedure will be made upon receipt of the expert report.
- Ongoing proceedings in Kavadarci involve the collection of material evidence, the details of which the prosecutor’s office cannot currently disclose.

The legal qualification for these criminal and legal events pertaining to the “Public Room 2” group will be determined based on the verbal and material evidence provided during the preliminary procedure.

Further cases involving public prosecutor’s offices throughout the country in instances where there is a well-founded suspicion of committing the criminal offense of Misuse of Personal Data under Article 141 of the Criminal Code, along with grounds for indictment and brief explanations of the offenses, can be found in Annex III.

5.2. Identifying inconsistencies in the judiciary and in the public prosecution in ensuring efficient justice for the protection of human rights, privacy, and ersonal data in the digital realm

Based on the analysis of court cases, the charges brought by the public prosecutor's office, and everyday instances we encounter, it appears that neither the authorities nor citizens have a comprehensive understanding of the rights related to the protection of personal data and privacy.

Let us begin with a review of the national legislation, specifically the Criminal Code. Article 149 prescribes the prohibition of personal data misuse and outlines corresponding penalties for violations of this legal provision. The penalty for unauthorized collection, processing, and utilization of personal data, whether in a general context or through computer information systems, is reduced to a fine or imprisonment of up to one year, which grants judges the discretion to impose penalties that often align with the legally mandated minimum, frequently resulting in suspended sentences. Our analysis of court cases suggests the following:

- Judges typically levy fines amounting to 30 daily fines, with one daily fine equivalent to MKD 615, resulting in a total fine of MKD 18,450 for personal data misuse.
- If judges opt for a suspended sentence, they often impose a prison term of three months, conditional on the individual refraining from committing new criminal offenses within a one-year period.
- Judges from the same court tend to impose identical sentences for the offense described in Article 149, paragraphs 1 and 2. For instance, the Basic Court Ohrid issue fines, while the Basic Court Strumica issues suspended sentences, etc.
- Sentencing for this crime varies across different courts, leading to a lack of uniformity in judicial practice.
- Smaller courts tend to impose higher penalties. For instance, the Basic Court Radovish imposed fines of 60 daily fines, equivalent to MKD

30,750, for an offense for which the Basic Court Ohrid levied a fine half the amount, under similar circumstances.

- Judges fail to classify the circumstances under the relevant paragraphs of Article 149 of the Criminal Code. For example, for an offense involving "recording the victim with his mobile phone, sharing the recorded video on the accused's, A.S., Facebook profile without the victim's consent, and subsequently leading to the victim's identification by their face", the verdict states that the accused committed an offense under Article 149 paragraph 1, instead of paragraph 2. The mitigating circumstance is that the penalties for both paragraphs are identical.
- The establishment of a legal practice favoring conditional fines for personal data protection abuses, as observed in the case of the Basic Court Kavadarci (K. No. 156/20), may hinder the realization of both specific and general deterrence.
- Public prosecutor's offices regularly respond to reports of personal data misuse, with particular attention given to cases drawing media scrutiny or involving foreign countries. The most common charges pertain to personal data misuse, enabling perpetrators to gain material or other benefit through bribery, blackmail, and similar means.
- In their notifications, in order to adhere to the principle of transparency, public prosecutor's offices provide brief announcements of ongoing preliminary investigations for specific cases, sharing that relevant documentation has been obtained without delving into case specifics, unless it pertains to a case of public interest.
- Macedonian citizens are vulnerable targets for fraudsters on social networks, who easily exploit personal data by creating fraudulent social network pages.
- A persistent and prominent campaign for personal data protection and the right to privacy is imperative!

5.3. Enhancing judicial capacity for merit-based decision-making in personal data protection and privacy, illustrated with ECJ jurisprudence

Beyond criminal and legal protection for personal data and privacy, the courts should also prioritize such protection within procedural proceedings. While the Law on Criminal Procedure has a dedicated section, other laws governing procedural actions, such as the Law on Litigation Procedure, the Law on Non-Contentious Procedure, and the Law on Family, lack provisions for such protection. However, there are no legal impediments to directly applying the provisions of the LPDP when the legal context demands it.

Even in EU member states, the extent to which national laws governing procedural actions need to align with national laws on personal data protection is not always clear. Consequently, judges often must exercise their discretion to determine how to safeguard privacy and prevent undue disclosure of personal data. This entails a careful assessment of proportionality and assessment of legal interest.

To ensure uniform application of the General Data Protection Regulation (GDPR) rules across the EU, the European Court of Justice (Court of the EU) has been involved in preliminary ruling procedures, offering authentic interpretation of specific GDPR provisions for national courts. This procedure is conducted following a question raised by a national court or tribunal of a member state, and the decision of the Court (ECJ) has legal force in all member states and it becomes a formal source of law.

While case law does not constitute a formal source of law in RNM, as a candidate country for EU membership and one fully compliant with the GDPR, such judgments hold utility and should be adequately translated and shared with judges, particularly through ongoing training.

I. Case C-268/21, Request for a Preliminary Ruling, Norra Stockholm Bygg AB v Per Nycander AB[42]

On March 2, 2023, the Court of Justice of the EU issued a ruling in case C-268/21, establishing that the GDPR applies to the generation of evidence in civil court proceedings. The case introduces certain limitations but does not exclude the generation of personal data within court proceedings.

The case revolves around a dispute between a construction company and its client regarding payment for completed construction works. The client (plaintiff) requested the Swedish court to compel the construction company to provide a copy of its electronic employee register, which contains, among other things, information about the identity of individuals involved in the construction works and their working hours—such registers are mandatory for construction companies under Swedish tax law. The amount of the compensation for the construction works was contingent upon on this data. The construction company contested the order, arguing that reusing the register in the context of a civil dispute conflicted with the original purpose of the register and therefore is impermissible under the GDPR. The Swedish Supreme Court referred the case to the ECJ for guidance on whether the GDPR applies to the generation of evidence containing personal data in court proceedings and whether national courts should consider the interests of the data subjects involved when assessing whether to order the generation of such evidence.

The ECJ ruled that the generation of evidence containing personal data, ordered by a court in the context of court proceedings, constitutes data processing under the GDPR. It concluded that in this case, securing the register through a court order served a different purpose (i.e., civil proceedings) from the original collection purpose (i.e., tax compliance).

However, the court deemed this “secondary use” of the register permissible under Article 6(1)(e), (3), and (4) of the GDPR, as it was mandated by national

42 Case C-268/21, available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62021CA0268.

or EU law that requires the protection of the purpose outlined in Article 23(1) of the GDPR. The court identified the proper administration of justice, such as submitting documents to the court, as one such goal. Consequently, national courts, when evaluating compliance with the GDPR in disclosing documents during court proceedings, should engage in a case-by-case assessment to determine whether the relevant provisions of national or EU law authorizing the disclosure align with one of the purposes outlined in Article 23(1) of the GDPR and whether they are necessary and proportionate to achieve those purposes. When only partial disclosure of personal data is justified, courts should consider data minimization measures like pseudonymization.

II. Case C-245/20, Request for a Preliminary Ruling, Rechtbank Midden-Nederland (District Court, Central Netherlands)[43]

In October 2018, during a court hearing in the Netherlands, Z (a party to the proceedings) and X (Z's representative) were approached by a journalist. In the course of their conversation, X noticed that the journalist possessed documents from the case file, including documents he had prepared himself, containing his name, address, and national identification number. The journalist asserted that he had obtained access to these documents under the right of access to case files, which the court had granted to him. This was confirmed in writing by the president of the court, who stated that he had provided the media with documents related to ongoing cases that journalists were covering on that particular day, including copies of the notice of appeal, response, and, when applicable, the disputed court decision, and journalists were instructed to destroy these documents at the end of the day once the proceedings had concluded. X and Z filed complaints with the Dutch data protection authority, which ruled that it lacked the jurisdiction to oversee the court's processing of personal data. Dissatisfied with this decision, X and Z challenged it before the District Court of the Netherlands, which then referred a preliminary ruling to the ECJ. The question revolved around whether Article 55(3) of the GDPR, which stipulates that "Supervisory authorities are not competent to supervise the processing processes of courts which act in their judicial capacities," implies

43 https://curia.europa.eu/juris/liste.jsf?language=en&td=ALL&num=C-245/20

that a court temporarily providing journalists with documents containing personal data from court proceedings is considered an act within the court‘s “judicial capacity.” In this context, the court sought clarification on whether it was necessary to assess the potential interference that the supervisory authority‘s exercise of its powers might have on the independence of judges in specific cases. Additionally, the court inquired whether it should consider the nature and purpose of granting access to procedural documents, i.e., allowing journalists to report on court proceedings, or whether such access must have an explicit legal basis in domestic law.

The ECJ ruled that the GDPR unequivocally applies to the procedural actions of the court, for example, Article 55(3), precludes the supervisory authority’s competence regarding processing operations conducted by courts “acting in their judicial capacities.”

Safeguarding the independence of the judiciary entails ensuring the full autonomy of judicial functions. Consequently, “acting in their judicial capacities” must be understood as extending beyond the mere processing of personal data in specific cases by the courts; instead, it must be broadly construed to encompass all processing operations conducted by courts in the course of their judicial activities.

Therefore, even if the nature and purpose of the processing conducted by the court primarily concern the examination of the legality of such processing, the nature and purpose may also suggest that the processing falls within the scope of the court’s “judicial capacity.

The ECJ opined that the decision whether to grant journalists access to documents in specific cases to facilitate accurate reporting on proceedings is directly linked to the exercise of the court’s “judicial capacities,” and oversight of this activity by an external authority could potentially undermine the overall independence of the judiciary.

Therefore, in line with Article 55(3), the ECJ ruled that a court temporarily providing journalists with documents from court proceedings containing

personal data to enable them to report on the proceedings is considered an action carried out within its "judicial capacity."

5.4. Relevant ECtHR judgments on personal data protection

As the Internet and digital communications continue to evolve, so do the rights of citizens. One noteworthy right is the "right to be forgotten," which empowers individuals to instruct information holders, such as internet search engines (e.g., Google, Yahoo, Bing, Mozilla), to remove web pages posted by third parties if their content infringes upon the honor, reputation, or privacy of individuals[44]. A landmark European case that established this right is the judgment of the Court of Justice of the EU in Luxembourg, case no. C-131/12 dated 13.05.2014[45]. In its judgement, the Court supported the decision of Spanish courts, which had ordered Google to remove specific content from its search engine, and the grounds for removal were that the content was "outdated and irrelevant" and violated the right to personal data protection.

The European Court of Human Rights (ECtHR), through its precedent-setting decisions, safeguards the right to privacy outlined in Article 8 of the ECHR, prescribing that every individual has the right to respect for their private life, and that there shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

44 Read more in Exercising the right to freedom of expression - theory and practice, IHR and CMC, 2017, p. 11-12. Available at:https://www.ihr.org.mk/storage/app/media/Publications/Pravo_na_slobodata_na_izrazuvanje_MK_web.pdf.

45 Google Spain SL and Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González. Link: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131.

Among the notable ECtHR judgments[46] are the following:

The right to a private life of a surrogate-born child (D.B. and Others v. Switzerland, nos. 58817/15 and 58252/15, § ..., 22 November 2022):

The case involved same-sex couples who were registered partners and had entered into a gestational surrogacy agreement in the United States of America, resulting in the birth of the third applicant. By a majority of six votes „for" and one „against," it was found that there had been a violation of Article 8. The general and absolute impossibility of obtaining recognition of the relationship between the child and the first applicant over a significant period of time constituted a disproportionate interference with the third applicant's right to respect for private life under Article 8. In this way, Switzerland exceeded its discretion by not adopting a timely legal provision for such a possibility.

Wiretapping of telephone communication in 2004 in the context of criminal proceedings (Potoczká and Adamčo v. Slovakia, no. 7286/16, §..., 12 January 2023):

The applicants, Anita Potochka and Branislav Adamcho, are partners, and the case concerns the wiretapping of telephone communication in 2004 in the context of the criminal proceedings for extortion against Mr. Adamcho. The tapped mobile phone belonged to Ms. Potochka, but – according to the authorities – was used by Mr. Adamcho. The court ruled that the interference with the applicants' right to respect for their private life and correspondence was not in accordance with the law. Hence, a violation of Article 8 of the Convention was established in relation to the two applicants.

46 Relevant judgments of the ECtHR in the field of protection of the right to personal data are available at: https://www.rolplatform.org/ и https://biroescp.gov.mk/%d0%bf%d1%83%d0%b1%d0%bb%d0%b8%d0%ba%d0%b0%d1%86%d0%b8%d0%b8/.

Systematic publication of personal data of tax debtors (L.B. v. Hungary [GC], no. 36345/16, § ..., 9 March 2023):

The case concerns the Hungarian legislative policy on the publication of the personal data of taxpayers who had tax debts. The applicant complained that his name and home address had been published on the list of "large tax debtors" on the website of the tax authorities in accordance with the 2006 legislative amendments to the relevant tax legislation. Legal amendments were made in 2006 in order to include tax debtors in the publication program (scheme). Specifically, section 55(5) was added to the Tax Administration Law of 2003, according to which the Tax Administration is obliged to publish a list of "large tax debtors", including the personal data of those whose tax debts exceed HUF 10 million in a period longer than 180 days.Право на политичарите на приватност (application no. 33776/20 Bojan Pajtić v Serbia, lodged on 13 July 2020, communicated on 10 November 2021)

Polititians' right to privacy (application no.33776/20 Bojan Pajtić v Serbia, lodged on 13 July 2020, communicated on 10 November 2021)

Although the ECtHR declared this appeal inadmissible, the case is still interesting for analysis. The applicant is a Serbian politician who held the position of President of the Provincial Government of the Autonomous Province of Vojvodina in the Republic of Serbia from 2004 to 2016. From 2014 to 2016, he was also the leader of the Democratic Party. At the outset, the Court reiterates that reputation is protected by Article 8 of the Convention as part of the right to respect for private life. However, for Article 8 to become applicable, the attack on a person's reputation must attain a specific threshold of gravity and be executed in a way that results in a violation of their personal enjoyment of this right. There was no contention that Article 8 was applicable in the particular case. Moreover, in situations where, as in the present case, Article 8 is invoked to safeguard "the reputation or rights of others,"

the Court may be called upon to ascertain whether the domestic authorities have effectively maintained a just equilibrium in safeguarding the two values enshrined in the Convention: namely, on one side, the freedom of expression safeguarded by Article 10, and on the other, the right to respect for private and family life as outlined in Article 8.

Right to privacy of a German actor (Axel Springer AG v. Germany (no. 2), no. 48311/10, § ..., 10 July 2014)

A German newspaper published photographs and reported on several occasions about an actor's association with drugs. In one specific report, three images were prominently featured on the front page. Subsequently, the actor initiated legal proceedings in Germany, where it was ruled that the actor's privacy had been violated by the publication of the images. The court banned the publication of the news and the images, which resulted in the newspaper being fined.

Unjustified processing of personal data of the applicants and disclosure of information about their health status (J.M. and A.T. v. North Macedonia no. 79783/13, § ..., 22 October 2020)

The applicants J.M. and A.T., who were patients at the Center for the Treatment of Addicts "S.E." within the Public Health Institution Strumica, claimed that their right to privacy had been violated because inspectors from the Department for Internal Affairs Strumica had accessed their medical records. In fact, following a prior report by the hospital due to a shortage and potential misuse of the sol.metadon solution, in April 2010, two inspectors from the DIA Strumica, without legal basis and without a court order, were granted access to and handed medical records containing the full names and quantities of methadone therapy received by patients, including both applicants. In June 2010, in response to the police's request, the hospital supplied copies of the aforementioned daily methadone distribution lists;

nonetheless, these copies did not include the patients' names and surnames. The police continued their investigation into the reported case, and in August 2010, they informed the Public Prosecutor's Office in Strumica that it had been determined there were no elements of a criminal offense concerning the missing methadone. Instead, it was deemed to be an error committed by an employee, and the medical records containing the personal data of both applicants were returned to the hospital. The court unanimously found a violation of Article 8 and determined that the domestic courts had not established a proper balance between protecting patients' rights and the police's right to access sensitive medical data without a court order.

Monitoring the use of the Internet by an employee at his workplace and using the data collected to justify his dismissal (Bărbulescu v. Romania [GC], no. 61496/08, § ..., 5 September 2017)

The applicant was dismissed by his private company employer due to the unauthorized use of the company's internet network during working hours, contrary to internal regulations prohibiting the use of company computers for personal purposes. For a period of time, the employer monitored the employee's communications on "Yahoo Messenger," which he had been instructed to open in order to respond to customer inquiries. The records obtained during the domestic proceedings showed that he exchanged messages of a purely private nature with other individuals. In the proceedings under the Convention, the employee claimed that the termination of his contract was based on a violation of his right to respect for his private life and correspondence, and that domestic courts failed to protect that right. The Court found a violation of Article 8.

Publication of the decision on the Commission's website on May 27, 2013, before its finality (Karajanov v. the former Yugoslav Republic of Macedonia, no. 2229/15, § ..., April 6, 2017)

On May 27, 2013, the Commission for the Verification of Facts ("the Commission") in a lustration procedure established that the applicant had collaborated with the State Security Services. Consequently, it decided that the employee met the conditions for restricting his candidacy and holding a public position. Based on another file no. 2599, the Commission found that, while serving as the chief editor of a newspaper in 1962 and beyond, the applicant had provided information to secret security services about his colleague, his colleague's articles, and his relationships with other individuals. The Commission's decision was published on their website on May 30, 2013. It contained information about the applicant's place of birth, identification number, and the roles he has performed. The decision was delivered to the applicant on June 4, 2013. The applicant complained that the publication of the decision on the Commission's website on May 27, 2013, before its finality, seriously damaged his reputation, dignity, and moral integrity, and violated his right to respect for his private and family life, in accordance with Article 8 of the Convention. The Court found a violation of Article 8.

Judgments from the European Court of Human Rights hold immense significance in establishing European legal standards and simultaneously provide valuable insights into the concept of privacy protection.

Пресудите на Европскиот суд за човековите права се од исклучително значење за формирање на европските правни критериуми, а истовремено се од голема помош за разбирањето на концептот на заштитата на приватноста.

5.5. Procedural and institutional strengthening of the judicial authorities in their role as controllers

The protection of personal data has specific characteristics depending on the nature of the roles involved. When acting in their judicial capacity, courts and prosecutors are subject to special requirements stemming from the nature of these roles and the need to uphold principles of independence and transparency. When acting in their judicial capacity, courts and prosecutors collect and process personal data to ensure proper conduct of court proceedings and to ensure that procedural documents are delivered to the parties in the proceedings. The processing is also intended to provide relevant information about the court proceedings, whether ongoing or closed, in accordance with the principle of transparent court proceedings. However, there are instances where judicial bodies are required to process personal data outside their judicial or prosecutorial capacity. For these reasons, it is necessary for courts and prosecutors to have their own rules for the protection of personal data when they act as controllers.

Courts maintain a large number of databases or case registries where personal information of parties involved is stored. The horizontal regulation governing the management of these databases and data entry is outlined in the Court Rules of Procedure, Official Gazette of the RM, No. 66, dated 9.5.201347. Regarding personal data in the Court Rules of Procedure, only the following articles apply:

- Article 287 on the Disclosure of data from the criminal records, according to which data from the criminal records can only be disclosed under the conditions prescribed by law, based on requests submitted in accordance with the provisions of the Criminal Code and the Rules of Procedure.
- Article 288, which stipulates that if a citizen requests data on convictions or non-convictions to exercise rights abroad, they must specify the rights they intend to exercise abroad in their request, and

47 Court Rules of Procedure, available at https://www.pravda.gov.mk/upload/Documents/sudski_delovnik_2014.pdf

- Article 130 on the anonymization of decisions, according to which an authorized judicial official, after receiving notification through the automated computer system for case management that a decision has been verified and sent to the parties (at first-instance courts) or to lower-instance courts (at higher-instance courts), must anonymize such a decision (final or non-final) within 2 days and publish it on the court's website in accordance with the Law on Court Case Flow Management and the issued instruction on the method of publishing and searching court decisions on the court's website.

Considering that the courts share a common website, the Judicial Portal of the Republic of North Macedonia www.vrsm.mk, the Court Rules of Procedure has not been published on it, nor is there a privacy policy or data protection policy.

In the section of published documents, a few case-laws on privacy and personal data protection have been published, issued by the President of the Basic Court Ohrid, representing a privacy policy of the Basic Court Ohrid[48]. It is recommended that such regulations be adapted and applicable to all courts, especially since the portal is managed by the Supreme Court of the Republic of North Macedonia; the privacy policy of the courts should be issued by the Supreme Court.

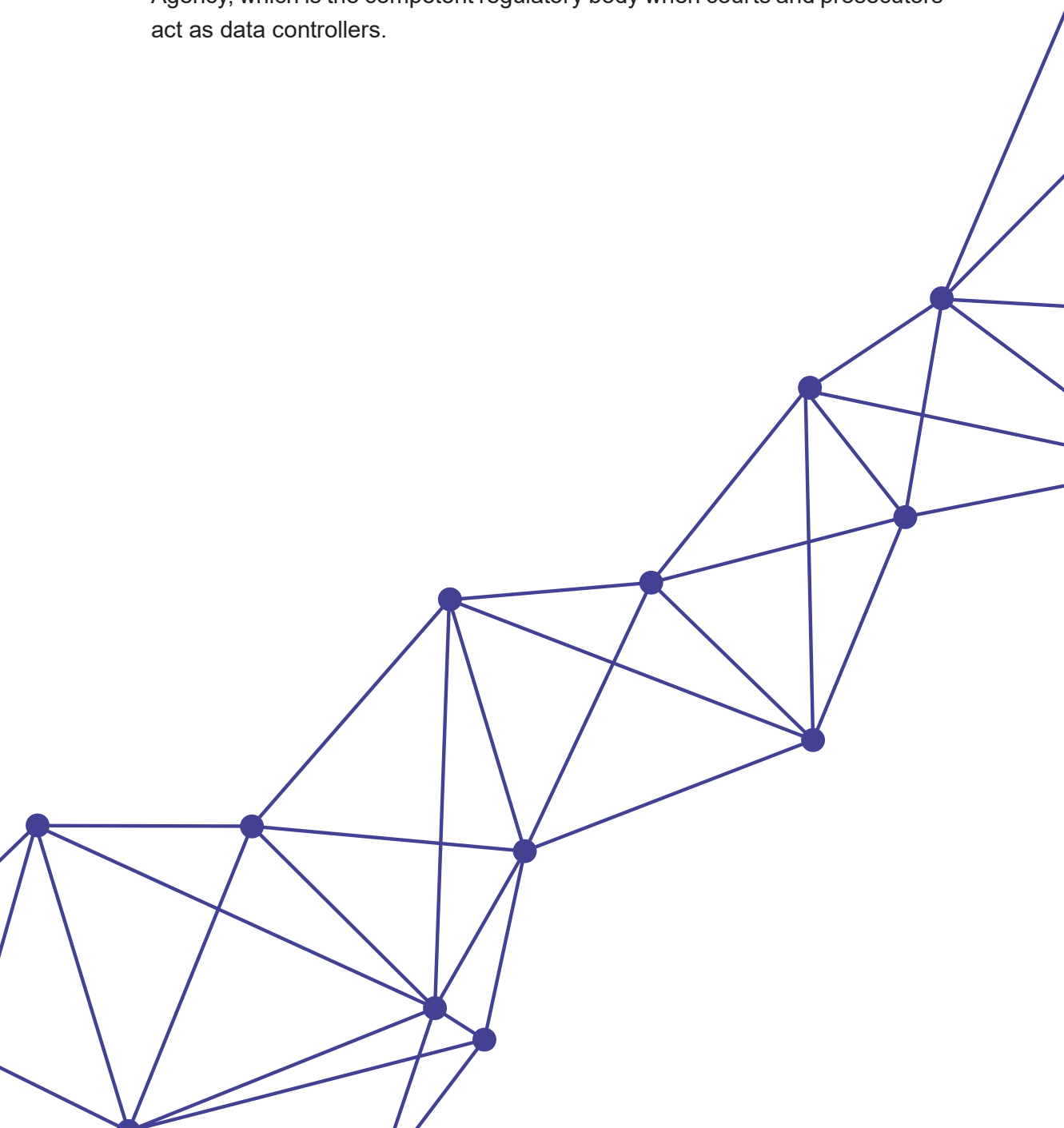
In terms of institutional strengthening for privacy policies and personal data protection, a training plan in this area has also been announced only for the Basic Court in Ohrid[49]. The annual plan includes training for the Data Protection Officer and training for the President of the Court and the judges in the Basic Court Ohrid.

The general recommendation here is to raise awareness about the need for personal data protection, and such training should be conducted for all

48 Rulebook on the technical and organizational measures to ensure secrecy and protection of the processing of personal data
49 Procedure for granting user privileges for authorized persons who process personal data

judges, that is, to be included in the training calendar for judicial officials for the current year.

Data Protection Officers and other employees in the judicial administration are required to attend training organized by the Personal Data Protection Agency, which is the competent regulatory body when courts and prosecutors act as data controllers.



VI.
CONCLUSIONS AND RECOMMENDATIONS

6. Conclusions and recommendations

1. Enhancing the legal framework for personal data protection, especially aligning sectoral legislation

This analysis identifies laws related to personal data protection and privacy. However, considering that personal data touches all aspects of life and is a complex matter, it is necessary to further identify sectoral legislation that requires alignment with the provisions of the LPDP. The Personal Data Protection Agency has signed a memorandum of cooperation enabling the alignment of sectoral legislation with the LPDP. For (proposers) ministries that are required to align their legislation with the Law on Personal Data Protection and for the necessary steps to synchronize their procedures with the law, the Agency has developed a Methodology for Sectoral Legislation Harmonization. This methodology provides instructions on how these proposers (ministries) should proceed to align their laws with the Law on Personal Data Protection and offers guidance on assessing the impact of these laws on personal data protection. The primary recommendation from the Agency is for ministries to first identify the laws that need to be amended or supplemented to align them with the LPDP and to utilize the opportunity for prior consultation with the Agency in the process of preparing new legislation.

2. Increased accountability of data controllers

The Agency and its role are widely recognized in the public, as evidenced by the Reports of procedures and requests for protection addressed to the Agency. An additional challenge is the role of data controllers, who are obligated to report to the Agency whenever there is a breach of personal data security. According to the Agency's data, there is a significantly higher number of reports compared to the number of notifications of breaches of personal data security by data controllers received by the Agency. Reporting is a legal obligation for data controllers (within 72 hours), and it requires additional effort to raise awareness about the necessity for data controllers to fulfill this legal obligation in a timely and regular manner.

3. Addressing the trend of increasing privacy breaches and guidelines/conclusions for improving standards and safeguards

Personal data protection constitutes an integral part of a society's culture. As citizens, we often overlook where we disclose our personal data and whom we entrust with personal documents containing such information, in pursuit of completing tasks or obtaining services. The realization of consequences typically dawns upon us only after it's too late, and our data has been exploited. To foster a more robust culture of safeguarding privacy and personal data, there is a pressing need for heightened public awareness campaigns and events featuring tangible examples from daily life.

4. Need to enhance the security of institutional IT systems (following specified instances of cyberattacks)

Recognizing the role of MKD-CIRT and establishing cooperation and connections between institutions and MKD-CIRT, both as its constituents and operators of critical infrastructure, is imperative. This holds particularly true for larger data controllers as one of the ways to bolster the security of institutional IT systems.

5. Conclusions concerning frequently filed charges

Of notable significance in this analysis is the substantial count of 232 complaints linked to social networks in 2022. Based on the reported reasons, the most prevalent complaints pertain to individuals reporting fake profiles, followed by cases involving unauthorized access to personal profiles (hacking), the publication of third-party's photos, video and audio recordings on third-party's social media profiles, and complaints involving online insults, defamation, and blackmail. When categorizing these complaints by the specific social network implicated, the majority are related to Facebook (116), then Instagram (103), and a subset of complaints (18) is linked to YouTube,

TikTok, Twitter, Snapchat, etc.[50] Consequently, it can be inferred that the most common charges pertain to personal data misuse, enabling perpetrators to gain material or other benefit through bribery, blackmail, and similar means.

6. Conclusions regarding judicial and prosecutorial efficiency

There is an imperative need to enhance the capabilities of judges and prosecutors in handling cases involving the protection of personal data. Resorting to imposing lenient sentences does not serve as a deterrent for offenders, as indicated by the growing number of reports, highlighting the frequent occurrence of these offenses. Capacity building, especially within the courts, is essential to uphold personal rights during legal proceedings where courts operate within their judicial capacity. The rulings of the European Court of Justice affirm that, in the absence of explicit regulations, judges frequently find themselves in the position of evaluating and determining the extent to which they will facilitate the protection of personal data in relation to other rights. Furthermore, the European Court of Human Rights has a corpus of judgments that can offer guidance or serve as a valuable resource for judges in their decision-making processes. Continuous training for judges and prosecutors is essential, given the dynamic nature of this field, which evolves in tandem with the online landscape itself.

7. Need for procedural and institutional strengthening of the judicial authorities in their role as controllers

The recommendations for judicial authorities regarding the need to strengthen capacities for personal data protection align with those applicable to all other data controllers. These authorities maintain substantial repositories of personal data and records. Ensuring the enactment of adequate privacy policies and legislation to guarantee data security is imperative, encompassing aspects such as authorized access, storage, anonymization, deletion, and more. The absence of regulations at both the court and prosecutor's office levels reflects

50 Personal Data Protection Agency, 2022 Annual Report, p.18. Link: https://azlp.mk/wp-content/uploads/2023/.

the need for uniform practices concerning this issue. Adequate training is essential, not only for personal data officers but also for administrative staff who work with such data.

ANNEX I
List of draft laws, by-laws and other materials for which the PDPA has provided an opinion

Year	Regulation	Ministry
2022	Draft Law Amending the Law on Border Control	Ministry of Interior
	Draft of the Agreement between the Government of the Republic of North Macedonia and the Government of Romania on strengthening cooperation in the field of internal control, and preventing and combating corruption	Ministry of Interior
	Draft Law Amending the Law on Foreigners	Ministry of Interior
	Draft Law Amending the Law on Child Protection	Ministry of Labour and Social Policy
	Draft Law Amending the Law on Social Policy	Ministry of Labour and Social Policy
	Draft Law on Asset Recovery Office	Ministry of Justice
	Draft Law on Criminal Procedure	Ministry of Justice
	Draft Law Amending the Law on the National Bank of the Republic of North Macedonia	Ministry of Finance
	Draft Law Amending the Law on the Public Revenue Office	Ministry of Finance
	Information regarding the announcement of a service on the interoperability platform for accessing data from the Ministry of Transport and Communications' transporter database, designed for use by control authorities and citizens during monitoring activities	Ministry of Transport and Communications
	Information on the public announcement of casefiles for the selection of elected/appointed officials of the Government of the Republic of North Macedonia as heads of institutions	Government of the Republic of North Macedonia

	Information on improving the transparency and accountability of the public sector institutions through the publication of mandatory information in accordance with the Law on Free Access to Public Information on the institutions' websites, as well as the publication of the most frequently requested information systematized by area and the draft conclusions in relation to it	Government of the Republic of North Macedonia
	Information on the state of affairs and the needs for improvement of the Crisis Management System concerning the management of wildfires	Government of the Republic of North Macedonia
	Rulebook on the method and conditions for performing video surveillance in penal and correctional institutions	Ministry of Justice, Office for the Execution of Sanctions
	Draft of the Decree on the organization and functioning - the establishment of a unified communication-information system featuring a single emergency hotline number for reporting risks, dangers, and other accidents across the entire country's territory (E-112)	Влада на Република Северна Македонија, Центар за управување со кризи

ANNEX II
Charges filed for misuse of personal data [51]

Public Prosecutor's Office	Grounds	Offense
BPPO Gostivar	Misuse of personal data under article 149 paragraph 1 of the CC	The suspect, without consent, on May 14 and 15, 2021, on several occasions downloaded photos from the Facebook profile of the victim's minor daughter and uploaded them on her personal profile. She added indecent and false comments to the photos taken in this way, which caused a feeling of humiliation in the victim and her daughter.
BPPO Skopje	Blackmail and misuse of personal data under article 149 paragraph 1 of the CC	The suspect, with the aim of acquiring financial benefit, blackmailed his ex-girlfriend by threatening to potentially publish her intimate photos on a social media platform. The suspect partially published the photos made while they were in a sexual relationship, after which he told the victim that if she did not give him MKD 5,000, he would publish the photos in their entirety.After reporting the blackmail to the police station, the victim gave the suspect a sum of money with traceable banknotes provided by the law enforcement, at an arranged meeting, after which the suspect was apprehended and taken into custody.
BPPO Gostivar	Misuse of personal data under article 149 paragraph 1 of the CC	During the month of August 2019, the accused, a 26-year-old man from Vrapchiste, misused the personal data of two victims. Without their consent, he opened profiles with their name on the Instagram social media platform and put personal data and photos of the victims on those profiles, in order to harm their dignity and reputation.
BPPO Skopje	Forgery of documents	BPPO Skopje initiated a case regarding the incident involving purportedly forged ID cards. During this process, a preliminary investigation was conducted to gather pertinent written documentation and essential data. Investigative actions are currently in progress; all steps taken during the preliminary investigation by either the public prosecutor or the police are treated as confidential.

51 The above procedures for misuse of personal data are available on the PPORM website, https://jorm.gov.mk/?s=%D0%BB%D0%B8%D1%87%D0%BD%D0%B8+%D0%BF%D0%BE%D0%B4%D0%B0%D1%82%D0%BE%D1%86%D0%B8.

BPPO Skopje	Dissemination of racist and xenophobic material through a computer system under art. 394-d. para. 1 of the CC, one criminal offense - Blackmail under art. 259 para. 1 in cojnjuction with art. 19 of the CC, one criminal offense - Piracy of an audiovisual work under art. 157-b para. 2 in conjunction with art. 1 of the CC and criminal offense - Misuse of personal data under art. 149 para. 1 of the CC.	The case was initiated following the filing of criminal charges against the defendant by multiple victims in 2022 and since the early part of 2023. These charges are linked to content published on a web portal owned by the defendant. Additionally, in an attempt to influence the ongoing proceedings against him, the defendant disclosed and disseminated personal data and photographs of four BPPO Skopje investigators without their consent. Consequently, the defendant also faces charges related to the criminal offense of Misuse of personal data.
BPPOPOCC	Fraud and Misuse of personal data	The group members, acting as agents, approached individuals across different domains, giving the impression that they were involved in trading various financial instruments, notably binary options, CFDs, Forex, and cryptocurrencies. They employed techniques such as affiliate marketing and manipulative advertising to entice numerous customers into completing contact forms, where they provided their personal data.
BPPOPOCC	Trafficking in human beings,	An organized criminal groupknown as the “Unions” lured individuals in Taiwan with promises of improved employment opportunities and an enhanced quality of life. To facilitate the bureaucratic processes related to travel, the victims’ travel documents were seized, and once they arrived at their destination, their mobile phones were also seized. The victims were then placed in residences where they were under constant supervision by one of the organizers, in order to restrict their ability to communicate with the outside world. The “operators” in the first level, in their interactions with the victims portrayed themselves as representatives from a bank, postal service, or insurance company. Then, in the second level, in an effort to acquire comprehensive personal data, they assumed the roles of police officers and demanded proof of payment for a fabricated fine, which served as a pretext to steal the victims’ personal data. The “operators” in the third level, impersonating prosecutors and judges, coerced the victims into believing that they would face serious charges unless they complied and transferred a specific amount of money to accounts. This payment was presented as a way to potentially reduce or avoid punishment.
BPPO Skopje	Production and distribution of child pornography under Article 193-a paragraph 3 in conjunction with paragraph 1 of the Criminal Code. Misuse of Personal Data	Between 19.12.2019, and 28.01.2020, the two suspects, who served as the founders and moderators of the group, were tasked with overseeing the textual and audio-visual content shared by group members. However, they intentionally permitted the dissemination of content within the group, including audio-visual material depicting explicit exual acts involving a child.

BPPO Gevgelija	Fraud under Article 247 paragraph 1 in conjunction with Article 45 paragraph 4 in conjunction with paragraph 1 and Misuse of personal data under Article 149 paragraph 1 in conjunction with Article 45 paragraph 1 of the Criminal Code.	Between 28.10.2019, and 2.2.2020, the suspect intentionally carried out a series of time-related actions, amounting to 18 instances of repeated commission of the same crime. With an intention to illicitly gain personal financial benefit, he was making phone calls to multiple elderly individuals, falsely identifying himself as an employee working for the Pension and Disability Insurance Fund or other state institutions involved in public interest activities. Through the presentation of misleading information, he manipulated and deceived the victims, leading them to believe that he could assist them in obtaining certain entitlements or pension benefits. To promise them a pension supplement, unpaid pension arrears from their spouses, suspension of legal actions, or other entitlements, the suspect requested the victims to furnish him with their personal data and documents, as well as to provide him with money for his supposed services. Through fraudulent means, the suspect successfully misappropriated MKD 54,650.00 for himself out of the agreed total of MKD 112,840.00.
BPPO Skopje	Manufacturing and procurement of weapons and means intended for the commission of a criminal offense under Article 395, Forgery of documents under Article 378 and Misuse of personal data under Article 149, all of the Criminal Code.	In the so-called case Factory for Affairs, the suspect is accused of having committed three criminal offenses, namely – Manufacturing and procurement of weapons and means intended for the commission of a criminal offense, Forgery of documents and Misuse of personal data.
BPPO Gostivar	article 353 paragraph 1 in conjunction with article 45 of the Criminal Code	Exploiting an ongoing, established relationship and leveraging available opportunities, the defendant, in violation of the provisions of the Law on Personal Data Protection and the Law on Civil Registry, issued one marriage register extract and three birth register extracts even though the defendant was fully aware that the recipient of these documents was neither a legal representative nor authorized proxy for the individuals mentioned in the documents. In this act, the defendant misused his official position and unlawfully disclosed and provided access to the personal data of the individuals mentioned in the records.

ANNEX III
Analysis of judgments from the Basic Court regarding the misuse of personal data [52]

Year	Basic court	Article/ praragraph	Grounds	Sentence
06.04. 2023	BC Radovish	Art.149 par.1	In August 2022, in R., the defendant violated the conditions set forth by the Law on Personal Data Protection. Specifically, after obtaining a photo of the identity card belonging to the victim, Z. U., from R., and forwarding it to his phone via the "Messenger" social network without Z.'s consent, the defendant visited a sales outlet of the mobile operator M. t. AD S. in B. There, he utilized Z.'s personal data, including her name, surname, and personal identification number, to enter into a sales contract and acquire a Samsung Galaxy A13 Black mobile phone. The device was delivered to him by a sales agent in R.1.	Fine MKD 30,750
22.11. 2022	BC Ohrid	Art.149 par.1	In the period from 06.02.2019 to 07.02.2019, in O., at his residence at 68 Klenoec Street, the defendant, in violation of legal provisions and without the consent of the victim, Lj.S., engaged in the unauthorized collection, processing, and utilization of her personal data. Initially, the defendant used the victim's personal data to create a profile on the social network "Facebook" under the name of the victim, specifically as "L... D... B...". Subsequently, he composed messages from this profile, which were sent to her relatives and friends. These messages contained inappropriate and offensive comments, sent under the guise of the victim herself.	Suspended sentence
29.09. 2022	BC Ohrid	Art.149 par.1	In November 2021, in O., at his residence on "..." St. no…, the defendant acted against the conditions stipulated by the law. Without the consent of the individual involved, namely, the victim D.M., who was his wife at that time while divorce proceedings were ongoing for their marriage, he gathered and utilized her personal data, namely: personal photos depicting the victim, and using his ST brand smart TV with the serial number ST-32TE4700 and the "Facebook" application installed on the TV, the defendant proceeded to create a Facebook account under the name "S... O..." with the following link: https://www.facebook.com/menka.menka.3...., and then on 12.11.2021, he utilized personal data in the form of a photograph featuring the victim, D.M., and publicly published it on the Facebook account "S... O..." along with a text that was publicly accessible.	Suspended sentence imprisonment for 3 (three) months (with 1 year)

52 The judgments are taken from the website of the Basic Courts, available at: http://www.sud.mk/wps/portal/.

16.09. 2022	BC Kichevo	Art.149 par.1	On 25.11.2019, in their capacity as the sole partner-owner and concurrently as the manager of the legal entity "V.. DOO Skopje from Skopje," the defendant misused the personal data of the victim, S. D. from K. The defendant, during the process of registering the aforementioned company in the Central Register of RNM, reported the personal address of the victim in K., specifically "…" St. no…., without obtaining the consent of the victim. This data, specifically the home address, falls under the category of personal data, as defined by Article 2 of the Law on Protection of Personal Data.	Fine MKD 18,450
16.08. 2022	BC Gevgelija	Art.149, para.1	The defendant, A.I., acted in violation of Article 5, paragraph 1, indent 1, Article 6, paragraph 1 of the Law on Protection of Personal Data. Specifically, on 03.02.2022, around 17:00, without obtaining the necessary permission and consent from the victim, S. T., the defendant used her personal data - her name and surname, in such a way that after she, as an authorized official, issued to him a misdemeanor payment order no. 259105 by PS ON G., he publicly published her data through his own profile on the social network "Facebook" in the group "Lafum givgiliski i ne sa zamarum", making them publicly available.	Suspended sentence imprisonment for 3 (three) months (with 1 year)
06.04. 2022	BC Ohrid	Art.149, para.2	On 18.10.2021 on the social network "Instagram" with the intention of using them for himself, contrary to Art. 10 para. 1 item 1 of the Law on Personal Data Protection (Official Gazette of RNM No. 42 of 16.02.2020) without previously obtaining consent for the processing of personal data (name, surname and photograph), which were the property of the victim E.P. from O., accessed the computer information personal data system, where he created a fake user profile with the name "e...", where he uploaded and processed photographs of the victim that she uploaded to her user profile and on the social network "Instagram".	Fine MKD 12,300
15.12. 2021	BC Bitola	Art.149 par.1	On 30.12.2020, contrary to the provisions set forth in Art. 9 and Art. 10 para. 1 of the Law on Personal Data Protection, without the consent of the victim V.V. from B. as a data subject, collected and processed the victim's personal data related to his physical identity, in such a way that during the verbal dispute in "N. p." in B. he recorded the victim with his mobile phone, and on the same day he shared the recorded video without the permission of the victim on the profile of the defendant A.S. on the social network Facebook, resulting in the victim being recognized by his face.	Fine MKD 18,450

19.08. 2021	BC Stip	Art.149 par.1	On 29.01.2020, contrary to the provisions set forth in the Law on Personal Data Protection, without the consent of the victim, Vlatko Keshishov from Sh., as a data subject, the defendant used his personal data - name and surname, personal identification number and bank account, in a way that, on the web platform DVLM-State Video Lottery of Macedonia Skopje for video lottery games of chance, he registered a profile - a game account with the name of Vlatko Keshishov with the ID....	Suspended sentence imprisonment for 4 (four) months (with 1 year)
10.05. 2021	BC Strumica	Art.149, para.1	In the period from 28.07.2019 to 20.08.2019, contrary to Art. 5 and Art. 6 of the Law on Personal Data Protection, without the consent of the victim, A.G from S., the defendant collected and utilized her personal data - photographs that the victim had previously posted, by creating a profile on a social network and with a username via a URL link, he misrepresented himself as the victim, and he published her photographs and communicated with third parties on her behalf, without her consent.	Fine MKD 30,850
26.04. 2021	BC Gostivar	Art.149 para. 1	During the month of A... in the year of …, contrary to the provisions set forth by law, without the consent of the victims M.Z. and M. H. from G., the defendant used their personal data in such a way that he opened profiles on the social network Instagram with the following names, namely, "l._..._mm,, ,,z.,, и ,,m..ii" with the victims' personal data and photographs, with the intention of harming their dignity and reputation.	Fine Anonymize
13.04. 2021	BC Gevgelija	Art.149 par.2	The defendant R.D. contrary to art. 6 para. 1 indent 1 of the Law on Personal Data Protection, on 23.06.2020, without the consent of the victim, K.T.-Deputy commander of the PS ON V, processed his personal data, a photograph of the victim that the defendant took from his profile on the social network Facebook, to which he attached a text with offensive and threatening content, and a misdemeanor payment order issued by another authorized official in the PS ON V, which the defendant published on the social network F. from his "R.D." profile and made them publicly available to all users of this social network, thus causing damage to the victim's professional authority and reputation.	Suspended sentence imprisonment for 3 (three) months (with 1 year)

11.03. 2021	BC Gostivar	Art.149, para.3	During the months of September and October... the defendant misused personal data in such a way that she opened a fake profile on the social network Facebook with the name A.A.J. and A.J.i and on the social network Instagram with the designation a..i. i a. on behalf of the victim A. from the village of K. -T. who is her former domestic partner.	Fine MKD 30,850
30.12. 2020	BC Kumanovo	Art.149 par.2	At an unspecified time in March 2018, in violation of legal provisions, the defendants, through the computer information system, accessed the personal data of the victim, M.T. - the principal of the secondary school "G. D." K., and the victims - students I.A., E.V., and S.D., with the intent to benefit themselves and others while causing harm to others. The first defendant published an article titled "Sex scandal in Kumanovo high school with photo evidence, everyone's getting busy with everyone, students, teachers" on his portal www.dokaz.mk through the computer information system. The second defendant, on the other hand, published an article titled "Scandal in a Kumanovo high school: students filmed pornographic films, the principal tried to cover up the case" on his portal "infomax.mk" through the computer information system. In these articles, the defendants disclosed the personal information of the victims, namely, their names, surnames, and professions. They also published explicit and compromising photographs of the student victims, suggesting that these photos were taken within the school premises. These actions were carried out with the intent to harm the dignity and reputation of the victim, as well as that of the students and the school itself, namely the Secondary school "Goce Delcev" K..	Released without charges
22.12. 2020	BC Stip	Art.149 par.1	On 05.07.2020 around 6:00, contrary to the provisions set forth in Art. 5 para. 1 and Art. 6 para. 1 of the Law on Personal Data Protection, without the consent of the victim S.A., as a data subject, the defendant used the victim's personal data, in a way that, while driving a BMV ... with reg. number ..., property of B.S., on the Sh.-Veles regional road, near the Tri Česmi settlement, was stopped by a police officer from the Ministry of the Interior-SVR Sh. for the purpose of carrying out traffic control, during which he was asked for personal identification documents, due to an ascertained violation under Art. 26 para. 1 and para. 10 of the Law on Vehicles, so instead of his own, he gave the personal data of the victim S.A. from K. born on 25.03.1989.	Fine MKD 18,450

14.09. 2020	BC Kavardaci	Art.149 par.1	On 06.05.2020, at approximately 17:30, in violation of Art. 18 of the Constitution of the Republic of North Macedonia and contrary to the stipulations of Art. 10 para. 1, and Art. 14 of the Law on Personal Data Protection, the defendant, without prior consent, made use of the personal data belonging to two citizens, namely, D.P. and T.Gj., both residing in K. The defendant carried out this action by publishing Criminal Verdict K. no. 62/20 dated 23.04.2020, from the Basic Court K. on his personal Facebook profile under the name "G.B." This verdict contained the personal data of the victims, including their name and surname, personal identification number, and residential addresses. Subsequently, there were various reactions from citizens in the form of comments and shares, effectively enabling an unauthorized and indefinite number of individuals to access the personal data of the victims.	Suspended fine A fine of MKD 18,450 that will be waived if no new offense is committed within one year
11.09. 2020	BC Strumica	Art. 149 para. 2 in conjunction with para. 1 of the CC	During the month of February 2020, the defendany accessed the computer information personal data system with the intention to cause damage to the dignity and reputation of the victim M.S., in such a way that without the knowledge and consent of the victim, from a computer in his home with IP address 89.185.194.48, he joined the social network Facebook and activated a profile in the name of his ex-wife M.S. with the username "Milka Gosheva", after which he published on his profile seven photos with inappropriate content depicting the victim.	Suspended sentence imprisonment for 3 (three) months (with 1 year)
14.07. 2020	BC Strumica	Art.149, para.1	During the month of March 2019, contrary to Art. 6 of the Law on Personal Data Protection, without the consent of the victim R.M. from Skopje, the defendant used his personal data by using the copy of the identity card to withdraw funds from a fast money transfer through Capital transfer Ria - Macedonia in S. Happy Car Wash DOOEL on 02.03.2019 with payment order DE 1483561037, on 06.03.2019 with payment order DE 1585051937, on 13.03.2019 with payment order DE 1755685137, on 15.03.2019 with payment order DE 1813658537 and on 16.03.2019 with payment order DE 183169937.	Fine MKD 61,500
02.06. 2020	BC Strumica	Art.149 par.1	In March 2019, in S., without obtaining the consent of the victim I.M. from S., the defendant violated Article 6 of the Law on Personal Data Protection by using the victim's personal data, which included their name, surname, address, personal identification number, and ID card number. The defendant then proceeded to fabricate a false document, namely a "Confirmation of regular employment" supposedly issued by the Company for production, trade, and services SOFI SOFIJA DOOEL import-export S., with archive number 215.2019 dated 04.03.2019. This fabricated document falsely indicated that the victim Ilija was employed in a regular capacity at DPTU SOFI SOFIJA DOOEL import-export S. Furthermore, on 04.03.2019, before the Company for Communication Services A1 Macedonia DOOEL S. at the time ONE.VIP DOOEL S., the defendant utilized this fraudulent document, presenting it as a genuine one. Under its guise, the defendant entered into an Agreement for establishing a subscriber relationship for the use of public telecommunication services, in the name of the victim I.M. from S. and ONE.VIP DOOEL S.	Suspended sentence imprisonment for 5 (five) months (with 1 year)

18.05. 2020	BC Strumica	Art.149 par.2	During the month of January 2020, the defendant accessed the computer information personal data system with the intention of causing harm to the victim M.Ch. in a way that by using two explicit photographs of the victim, which he had downloaded from her mobile phone and took a picture of her while they were talking through the M application, from his phone number through the W application, he sent the photos to the person T.Gj. from N S, without the victim's awareness or consent, thus making them accessible to a third party.	Fine MKD 18,600
04.05. 2020	BC Stip	Art.149 par.1	On 26.04.2019, in Sh., acting in collusion and jointly, the defendants, in violation of Art. 4 of the Law on Personal Data Protection, utilized the personal data of a citizen, namely the victim Z.V. from Sh., without obtaining his consent. This occurred after the victim had provided his identity card and debit card to the second defendant, for the purpose of seeking financial assistance for his medical treatment. Subsequently, the second defendant, using a photocopy of the victim's identity card and email address..., falsely applied for a fast online consumer loan at the Financial Company "Credissimo" in Skopje, under the name of the victim.	Suspended sentence imprisonment for 3 (three) months (with 1 year)
14.04. 2020	BC Ohrid	Art.149 par.2 of the CC	On 11.11.2019 in O., contrary to the provisions laid down in the Law on Personal Data Protection, without the consent of the victim I.. B.. from O., with whom they were previously in a romantic relationship, used her personal data, by publishing on the porn website Macedonian room- V.. & chat a video clip that I.. B.. had created herself by filming her torso without revealing her face. The defendant had received this video clip from the victim in a private message via the Instagram application on 14.12.2018. By publishing this video, the defendant caused intangible harm to the victim.	Fine MKD 12,300
30.12. 2020	BC Strumica	Art. 149 para. 2 in conjunction with para. 1 of the CC	The defendant A. using the copy of the identity card of the victim H.J. from S. which the victim sent to her through "messenger" on the social network F in November 2018 in order to make her a member of A K, on 26.12.2018, made an unauthorized access through the computer information system to the profile created on the name of the victim X on the website A. In the victim's name, the defendant placed an order for cosmetic products totaling MKD 6,000. Consequently, the victim, H, was left owing this amount for the products, while the defendant retained the products for herself.	Suspended sentence imprisonment for 3 (three) months (with 1 year)