A Guide to Protecting the Right to Privacy in the Digital Space

(Practical Guidelines for Legal Professionals)

January, 2024

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

IMPRESSUM

Title: A Guide to Protecting the Right to Privacy in the Digital Space

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

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

Author: Aleksandar Godjo

Contribution: Eva Suhrada Kirschmeier, PhD
Irena Bojadjievska, Assistant Professor
LL.M Milena Josifovska

Editing: Center for Legal Research and Analysis

Proofreading: Dejan Vasilevski

Graphic design: Vertigo

Editor: Lidija Stojkova Zafirovska

Print: Polyesterday

Circulation: 30

Place and year of publication: Skopje, 2024

The present 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 authors shall be solely responsible for the contents of the publication, and it may not be deemed in any manner to represents the views of the European Union.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

GDPR – General Data Protection Regulation

LPDP – Law on Personal Data Protection

CC – Criminal Code

LCP – Law on Criminal Procedure

LCP – Law on Civil Procedure

LO – Law on Obligations

LGAP – Law on General Administrative Procedure

LAD – Law on Administrative Disputes

EU – European Union

TAIEX – Technical Assistance and Information Exchange Instrument

ECtHR – European Court of Human Rights

ECJ – European Court of Justice

ECHR – European Convention on Human Rights

UNGA – United Nations General Assembly

ICT – Information and Communications Technologies

PDPA – Personal Data Protection Agency

MOI – Ministry of Interior

BPPO – Basic Public Prosecutor's Office

PPO – Public Prosecutor's Office

„PRIVACY IS NOT A PRIVILEGE, IT IS A FUNDAMENTAL HUMAN RIGHT“

VIVIANE REDING

INTRODUCTION

In lieu of an introduction, consider a single data point that unmistakably encapsulates the scale of the phenomenon we are discussing.

Based on a 2022 survey focusing on websites that also feature social media and have experienced the most substantial user data losses (refraining from delving into the fate of the data or the ensuing potential damages), the situation is as follows.

1. Yahoo - 3.5 billion

Over 3.5 billion users have been impacted by data breaches associated with Yahoo, with three billion individuals affected by the 2013 breach alone.

2. Facebook – 2.1 billion

In 2019, a series of four distinct breaches resulted in the compromise of data from over two billion Facebook users.

3. LinkedIn – 1.1 billion

The majority of LinkedIn's 1.1 billion users, whose data was disclosed, fell victim to a breach in 2021, culminating in the sale of 700 million data.

4. MySpace - 719 million

Those three breaches disclosed the data of 719 million MySpace users. The now-defunct site had just seven million users in 2019.

5. Sina Weibo - 538 million

In 2020, the data of 539 million users of the Chinese social media platform, including 172 million phone numbers, were made available for sale.

6. Twitter - 370 million

In June, Twitter verified that a hacker had accessed contact details for 5.4 million accounts, contributing to the overall count of affected users of the microblogging site.

7. Quora – 100 million

Quora, the question-and-answer platform, disclosed that a hack in 2018 led to the exposure of passwords and security questions for a hundred million users.

8. Dailymotion – 85 million

In a 2016 breach, a hacker stole over 85 million distinct email addresses and usernames from the video-sharing platform Dailymotion's systems, along with passwords for 18.3 million accounts.

9. Tumblr – 65 million

In 2016, Tumblr disclosed that its security had been compromised three years prior, leading to the unauthorized acquisition of user account information of 65 million people.

10. Instagram – 49 million

In 2019, approximately 49 million users of the Facebook-owned photo-sharing platform Instagram faced exposure when an unsecured server was leaked online.[1]

The digital transformation of our society stands as one of the swiftest and most profound transitions in civilization that we have ever encountered. In the digital age, our communication is increasingly shifting online—whether for information, entertainment, consumption, or work. The COVID-19 pandemic has revealed the potential of digital services, enabling individuals to sustain communication and engagement, and fostering increased resilience. However, numerous questions persist regarding the consequences of this transformation and its impact on human rights.

The issue of privacy has long held relevance in our daily lives, but the growing utilization of virtual space and advancements in technology, such as artificial intelligence, further brings these debates into the spotlight. Rather than mitigating discrimination or inequality, certain algorithmic decision-making systems have the potential to exacerbate these issues, particularly in the public sphere. The use of predictable features within the justice system seems to give rise to a new source of law. Facial recognition tools reintroduce concepts like physiognomy, resurrecting the belief that behavioral characteristics can be inferred from physical features.

The full enjoyment of our rights in cyberspace necessitates adequate protection from the risks present in the online environment. The right to private life, human dignity, security, personal integrity, and non-discrimination are jeopardized by the threat of cybercrime.[2]

1 https://businessplus.ie/tech/social-media-lost-user-data/

2 ECHR Symposium: Human Rights in the Digital Sphere

PURPOSE AND SCOPE

This guide is designed to serve as a practical tool consolidating essential concepts, legal frameworks, threats, principles, actors, mechanisms, legal remedies, and procedures outlined in the legislation and practice of the Republic of North Macedonia. Additionally, it will address certain practical dilemmas, and provide examples and rulings of the European Court of Human Rights and the European Court of Justice on these issues.

The examples and guidelines provided in this guide are intended to assist state authorities, particularly the PDPA, as well as judiciary actors (judges, public prosecutors, lawyers) in the Republic of North Macedonia, as well as all legal and natural persons, when dealing with data protection issues, whether overseeing or supervising the application of regulations, adjudicating complaints or lawsuits related to the handling, processing, or misuse of personal data, detecting and/or prosecuting perpetrators of criminal acts and offenses, providing legal assistance, or are obligated to respect personal data protection within the scope of their activities. Simultaneously, these examples and guidelines are highly recommended for all legal and natural persons, whether directly involved or obligated to adhere to the rules and regulations governing this sphere, to recognize the dangers and challenges and to skillfully utilize the available tools in order to safeguard themselves, minimize risks to their rights to privacy and protection of personal data in cyberspace, as well as to help them effectively utilize legal mechanisms and remedies within both the domestic and international legal order.

Key principles

The document is founded upon the key principles for the development of "A Guide to Protecting the Right to Privacy in the Digital Space", which were formulated through the TAIEX Expert Mission conducted in the Republic of North Macedonia from October 31 to November 2, 2023. The TAIEX mission aimed to offer assistance and guidance in the development of "Guidelines for Judicial Stakeholders on Privacy and Data Protection in the Republic of North Macedonia", in accordance with the GDPR and the EU acquis in this area.

The present document encompasses the recommendations, providing detailed elaborations for each.

Key definitions

For the purposes of this guide, our initial task is to define the fundamental terms that encapsulate the essence of the subject matter.

„Personal data"

encompasses any information pertaining to an identified or identifiable natural person ("data subject"). An identifiable natural person is someone who can be directly or indirectly identified, specifically by reference to an identifier like a name, identification number, location data, online identifier, or one or more factors unique to the physiological, genetic, mental, economic, cultural, or social identity of the natural person.

„Special categories of data"

refer to personal data that disclose information regarding racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, or data about the natural person's sex or sexual orientation. These categories are subject to a specific framework (Article 3 of the LPDP).

„Processing"

refers to any operation or series of operations carried out on personal data or collections of personal data, regardless of whether it is automated or not, such as collection, recording, organization, structuring, storage, adaptation or modification, retrieval, consultation, use, disclosure by transmission, dissemination, or any other form of making available, matching or combination, restriction, deletion, or destruction.

„Controler"

refers to a natural or legal person, public authority, agency, or any other entity which, independently or jointly with others, determines the purposes and means of the processing of personal data. Where Union or Member State legislation dictates the purposes and means of such processing, the appointment of the controller or the specific criteria for such appointment shall be outlined in Union or Member State legislation.

„Processor"

refers to a natural or legal person, public authority, agency, or any other entity that engages in the processing of personal data on behalf of the controller

„Recipient"

refers to a natural or legal person, public authority, agency, or any other entity to whom personal data is disclosed, irrespective of whether it qualifies as a third party. Nevertheless, public authorities acquiring personal data as part of a specific investigation under the law shall not be classified as recipients. The processing of such data by public authorities must adhere to the applicable data protection regulations, aligning with the purposes of the processing.

Cyberspace

The term was coined by the science fiction novelist William Gibson in 1984.

Cyberspace is the environment where human interactions take place over computer networks, via email communication, gaming, or simulations.[3] The term cyberspace is defined as (A) an interdependent network of information technology infrastructures and (B) encompasses the Internet, telecommunications networks, computer systems, as well as embedded processors and controllers.[4]

3 https://www.lexisnexis.co.uk/legal/glossary/cyberspace#:~:text=%27Cyberspace%27%20is%20where%20human%20interaction,through%20email%2C%20games%20or%20simulations

4 https://www.law.cornell.edu/definitions/uscode.php?width=840&height=800&iframe=true&def_id=50-USC-119985075-325479117&term_occur=999&term_src=title:50:chapter:35:section:1708

01
LEGAL FRAMEWORK

I.

LEGAL FRAMEWORK

In legal discourse, there is an ongoing discussion and a degree of confusion regarding the existence of a singular legal framework that may effectively integrate human rights, personal data, and cyberspace. Due to its cross-border and information-centric nature, cyberspace poses a challenge to the traditional governance approach of states. On one hand, the physical infrastructure constituting cyberspace falls under national jurisdiction and authority. On the other hand, the flow of data and information through that infrastructure may continually traverse (multiple) territorial jurisdictions, creating a challenge for any single jurisdiction to exert "effective control" over this information flow. This has prompted numerous calls for the establishment of new norms, advocating for the introduction of regulatory frameworks to govern the cyberspace.

In contemporary discussions, it is indisputable that the principles of international law should be applicable in cyberspace. The implementation of these principles into practice is less straightforward.

As a result, this disparity between policy and practice gives rise to legal uncertainties and even potential legal gaps, which can compromise the safeguarding of the human rights of internet users. In response, international and regional organizations have taken initiatives to identify and interpret the application of existing legal principles of international law in cyberspace.[5]

Nevertheless, there is an aspiration to incorporate new technological advancements into legal norms as much as possible, allowing for the regulation of the behavior. In the absence of detailed regulations, legal gaps are filled in accordance with the most closely related norm.

5 Guide to Good Governance in Cybersecurity, 2019, ©DCAF – Geneva Centre for Security Sector Governance, Geneva – 2019.

1.1. Domestic legal norms, Constitution, Law on Personal Data Protection, other Relevant Regulations

The domestic legal order is governed by the Constitution, as the highest legal instrument, as well as by various other laws.

The LPDP stands out as the legislation most directly addressing the issues outlined in this guide. Other procedural and substantive laws, including LCP, LCP, LGAP, LAD, the Law on Obligations, the Law on Electronic Communications, the Law on Media, etc., each contribute as integral components to the mosaic of personal data protection, the right to privacy, and human rights.

As per the Constitution[6], international instruments form an integral part of the domestic legal order and hold supremacy. They will be examined in the section dedicated to international legal instruments.

1.2. International Legal Instruments

1.2.1. Universal Declaration of Human Rights and International Covenant on Civil and Political Rights

It is widely acknowledged in the international context that international human rights law, encompassing the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, is applicable in the digital space. This was affirmed by the Human Rights Council (HRC) in resolution A/HRC/20/L.13, stating that "the same rights that people have offline must also be protected online". This resolution is significant as it marked the first instance where an international body explicitly declared that the safeguarding of human rights extends to the realm of cyberspace. In response to the Snowden revelations, the UNGA opted to establish a new Special Rapporteur on the right to privacy in 2015, aiming to enhance the addressing of privacy issues in the digital age and promote a safer digital environment. The Special Rapporteur on the right to privacy is tasked with conducting state visits, offering recommendations, and handling individual complaints.

6 Article 110. International agreements

REPORT OF THE UN GROUP OF GOVERNMENTAL EXPERTS

The 2015 UN report puts forth the following recommendations for responsible behavior by states to contribute to an open, secure, stable, accessible, and peaceful cyberspace:

POSITIVE NORMS:

- States should collaborate to enhance stability and security in the use of ICT and to prevent harmful ICT practices.
- States should consider all relevant information pertaining to attribution in the ICT environment.
- States should implement appropriate measures to safeguard national critical infrastructures from ICT threats and respond to relevant requests for assistance from another state.
- States should adopt reasonable measures to secure the integrity and mitigate the dissemination of malicious ICT tools and techniques.
- States should promote the responsible reporting of ICT vulnerabilities and dissemination of related information.

LIMITING NORMS:

- States should refrain from knowingly permitting their territory to be utilized for international and wrongful actions using ICT.
- States should adhere to United Nations General Assembly resolutions pertaining to human rights.
- States should refrain from knowingly supporting any ICT activity that contradicts their obligations under international law.
- States should refrain from engaging in or knowingly supporting activities aimed at harming the information systems of authorized emergency response teams.

1.2.2.Regulation (EU) 2016/679 (General Data Protection Regulation)

This regulation defines rules concerning the safeguarding of natural persons in connection with the processing of personal data and rules pertaining to the unrestricted movement of personal data. It safeguards the fundamental rights and freedoms of natural persons, with particular emphasis on their right to personal data protection.

In accordance with this Regulation, the unrestricted movement of personal data within the Union will not be constrained or prohibited on grounds related to the protection of natural persons in connection with the processing of personal data.[7]

This Regulation is applicable to the processing of personal data in the context of activities involving the establishment of a controller or processor in the Union, irrespective of whether the processing occurs within the Union or beyond its borders.[8]

1.2.3. UN Resolution on the Creation of a Global Culture of Cybersecurity

Another important UNGA resolution is A/RES/57/239 on the creation of a global culture of cybersecurity that recognizes cybercrime as a major cybersecurity challenge.[9]

1.2.4. United Nations Guiding Principles on Business and Human Rights

Furthermore, the United Nations instrument pertinent to the identification of norms in cyberspace is the United Nations Guiding Principles on Business and Human Rights (also recognized as the "Ruggie Principles"), adopted in 2011. These principles provide guidance to both states and businesses concerning the protection of human rights. The Ruggie Principles are founded on the UN framework of "Respect, Protect, and Remedy". The introductory section of these guiding principles asserts that "business enterprises, as specialized organs of society performing specialized functions, are required to comply with all applicable laws and to respect human rights".

In the realm of regulating specific manifestations of unlawful expression on the Internet, such as hate speech, the report of the UN High Commissioner for Human Rights, adopted by the Human Rights Council in 2013 (referred to as the "Rabat Plan of Action Plan"), outlines criteria for identifying hate speech and can offer guidance in the online domain as well.

1.2.5. European Convention on Human Rights

One of the most significant legal instruments of the 20th century, the Convention, provides a definition of the right to privacy in the context of modern times through its interpretation in Article 8. According to the ECHR, Article 8 and its interpretation encompass the scope where the right to the protection of privacy, personal data, and their utilization resides, including the safeguarding of rights in the online space. The Council of Europe relies on the ECtHR as the entity responsible for interpreting the convention and offering protection through individual applications. To invoke Article 8, the applicant must demonstrate that their application pertains to at least one of the four interests specified in the Article, namely: private life, family life, home, and correspondence.

Certainly, certain matters may involve multiple interests. Initially, the Court assesses whether the applicant's application falls within the scope of Article 8. Subsequently, the Court examines whether there has been interference with that right or if the state's positive obligations to safeguard the right have been triggered. The circumstances under which the state may interfere with the enjoyment of the protected right are delineated in paragraph 2 of Article 8. These include the interest of national security, public safety,

7 Regulation (EU) 2016/679 (General Data Protection Regulation), Article 1.

8 Ibid., Article 3.

9 https://documents-dds-ny.un.org/doc/UNDOC/GEN/N02/555/22/PDF/N0255522.pdf?OpenElement

or the economic well-being of the country, prevention of disorder or crime, protection of health or morals, or to safeguard the rights and freedoms of others. Restrictions are permissible if they are "in accordance with law" or "prescribed by law" and are deemed "necessary in a democratic society" to protect one of the aforementioned purposes. In evaluating the test of necessity in a democratic society, the Court frequently encounters the need to balance the interests of the applicant protected by Article 8 against the interests of third parties protected by other provisions of the Convention and its Protocols.[10]

1.2.6. Council of Europe Convention on Cybercrime

The need to harmonize and systematize substantive and procedural norms globally in the realm of cybercrime and electronic evidence has been expressed in the Convention on Cybercrime of the Council of Europe, hereinafter referred to as "the Convention". While prior attempts had been made to define the substantive norms governing international legal cooperation, the Convention, characterized by its comprehensive nature, flexibility, and ease of incorporation into national legislation, has evolved into a recognizable mechanism facilitating communication not only among European states, its original target, but also among states worldwide.

The Convention on Cybercrime was subsequently accompanied by the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data[11], along with amendments and the Additional Protocol regarding supervisory authorities and transborder data flows[12], the Additional Protocol to the Convention on Cybercrime covering the protection against racism and xenophobia[13], the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse[14], and EU Directives.

The Convention on Cybercrime was adopted by the Council of Europe in Budapest on November 23, 2001. A total of 58 countries have signed the Convention, with 28 having subsequently ratified it. Our country signed the Convention on November 23, 2001, ratified it on September 15, 2004, and it came into force on January 1, 2005.

The Convention encompasses substantive, procedural, and international cooperation norms. Substantive law provisions pertain to unauthorized access, unauthorized interception, data intrusion, system intrusion, device misuse, computer-related forgery, computer-related fraud, offenses related to child pornography, copyright infringement, and infringement of other related rights.

In accordance with the Explanatory Protocol to the 2001 Convention on Cybercrime, swift advancements in information technology have a direct impact on all facets of modern society. The integration of telecommunications and information systems facilitates the storage and transmission of all forms of communication, regardless of distance, thereby unlocking a vast range of new possibilities. These advancements have been propelled by the emergence of information superhighways and networks, including the Internet, providing virtually anyone with the ability to access any electronic information service, regardless of their location. Through communication and information services, users establish a shared space known as "cyberspace", utilized for legitimate purposes but susceptible to misuse, including breaches of the confidentiality of computer systems and telecommunications networks, or the utilization of such networks and services to commit traditional offenses. The transboundary nature of these offenses, for instance, when carried out over the internet, clashes with the territorial jurisdiction of national law enforcement authorities.[15]

1.2.7. Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data

According to the Explanatory Memorandum to this Convention, the right to respect for family and private life is stipulated in Article 8 of the ECHR. This right is further interpreted through the jurisprudence of the Court and is reinforced and augmented by Council of Europe Convention 108.

Private life is a concept that is not subject to an exhaustive definition. The Court emphasized that Article 8 encompasses a broad spectrum of interests, namely private and family life, home, and correspondence, which includes post, telephone communications, and email in the workplace. Privacy encompasses an individual's right to their own image, as seen, for example, in photos and video clips. Privacy also pertains to an individual's identity and personal development, and the right to establish and cultivate relationships with other human beings. Professional and business-related activities also fall within the scope of privacy.

10 https://www.echr.coe.int/documents/d/echr/guide_art_8_eng

11 https://azlp.mk/wp-content/uploads/2022/11/Zakon_za_ratifikacija_na_Konvencijata_108.pdf

12 https://azlp.mk/wp-content/uploads/2022/11/Dopolnitelen_protokol_Konvencija_108.pdf

13 https://www.pravdiko.mk/wp-content/uploads/2013/11/Dopolnitelen-protokol-na-Konventsijata-za-kompjuterski-kriminal-za-inkriminatsija-na-dela-od-rasistichki-i-kesnofobistichki-vid-ETS-189.doc

14 http://www.childrensembassy.org.mk/WBStorage/Files/Konvencija%20na%20Sovetot%20na%20Evropa%20za%20zastita%20na%20deca%20od%20seksualna%20zloupotreba.pdf

15 https://rm.coe.int/16800cce5b

02

RIGHT TO PRIVACY AND DATA PROTECTION

II.

RIGHT TO PRIVACY AND DATA PROTECTION

Examining these two terms, they are not synonymous. In practice, there are numerous debates surrounding the nuances of these two rights. One thing is evident: the right to privacy is a more encompassing concept than data protection.

2.1. Right to privacy

Privacy is not solely an individual right but also a societal value. It is ingrained in the concepts of individualism, freedom, and the right to the protection of the individual. In some countries, such as the USA, privacy is frequently regarded as an aspect of freedom, representing the right to be free from intrusions by the state. Privacy is a fundamental right, acknowledged in almost all countries worldwide, either through constitutional provisions or other legal frameworks as the right to privacy is enshrined in the Universal Declaration of Human Rights (Article 12), the European Convention on Human Rights (Article 8), and the European Charter of Fundamental Rights (Article 7).

One obvious difference lies in the fact that privacy is acknowledged as a universal human right, whereas data protection is not (at least not yet).[16]

2.2. Concept of data protection

Data protection pertains to safeguarding any information concerning an identified or identifiable natural person, including names, dates of birth, photographs, videos, email addresses, and telephone numbers. Additional information, including IP addresses and communication content that is linked to or provided by end users of communication services, is also considered personal data.

The concept of data protection originates from the right to privacy. Both are instrumental in preserving and promoting fundamental values and rights, and they contribute to the exercise of other rights and freedoms, such as freedom of speech or the right to assemble.

Data protection has specific objectives to ensure the fair processing (collection, use, storage) of personal data by both the public and private sectors.[17]

16 https://edps.europa.eu/data-protection/data-protection_en
17 Ibid.

2.3. Protection against indirect identification

It is crucial for all the actors mentioned in this guide, who work with or have contact with data, to understand that the information they possess can lead to the indirect identification of a specific individual. Therefore, even seemingly indirect or secondary data should be treated as personal data. Thus, they are subject to the protection framework outlined in the GDPR/LPDP.

If an individual cannot be directly identified from the information processed by the professional (for example, when all identifiers are removed), it does not preclude the possibility of identifying the individual through other means, such as information previously held by the professional (the one utilizing or processing such data) or information they are expected to receive from another source. Likewise, a third party could utilize the information held by the professional, and when combined with other available information, this process may result in the identification of the individual.

In such a case, the responsibility for assessment lies with each actor mentioned in this guide. They should evaluate which information is likely to be used for processing and which could lead to the identification of the individual in order to prevent inadvertently publishing or disclosing information that could be linked to other data and (inappropriately) identify the individual.

What types of information have the potential to indirectly disclose the identity of an individual?

While there is no exhaustive list, a combination of the following types of information can potentially lead to the identification of an individual:

- vehicle registration number,
- passport number, or
- a combination of significant criteria (e.g., age, occupation, place of residence).

The crucial aspect of indirect identification occurs when information is combined with other information, creating distinctions that facilitate the identification of an individual.

2.4. Right to data protection

Privacy and data protection are two rights enshrined in the EU Treaties and the EU Charter of Fundamental Rights.[18] The Charter explicitly includes the right to the protection of personal data (Article 8). The entry into force of the Treaty of Lisbon in 2009 bestowed upon the Charter of Fundamental Rights the same legal standing as the EU constitutional treaties. Consequently, the institutions and bodies of the EU, as well as the Member States, are obligated to adhere to it. Additionally, Article 16 of the Treaty

18 https://edps.europa.eu/data-protection/data-protection_en

on the Functioning of the European Union (TFEU) mandates the EU to establish data protection rules for the processing of personal data. The EU is unique in stipulating such an obligation within its constitutional framework.

2.5. Personal data protection regulations

In April 2016, the EU adopted a new legal framework – the General Data Protection Regulation (GDPR) and the Data Protection Directive for law enforcement and the police.

Enforced throughout the EU as of May 2018, the GDPR stands out as the most extensive and forward-thinking legislation on data protection globally, updated to address the challenges brought about by the digital era.

The Republic of North Macedonia has transposed this regulation through the adoption of the LPDP.

03
HORIZONTAL APPROACH

III.

HORIZONTAL APPROACH

Data protection is a horizontal issue, implying that within each distinct sector, the Law on Personal Data Protection (LPDP) should be considered in addressing any legal issue that requires resolution. Moreover, regulations incorporating sector-specific data protection provisions (such as law on telecommunications, law on e-commerce, media law, etc.) should also be taken into consideration and applied accordingly. These regulations must also be considered when addressing a particular legal situation.

In addition to laws, when assessing cases pertaining to data protection, consideration will be given to the jurisprudence of the European Court of Human Rights (ECtHR), taking into account our country's aspirations towards the European Union, as well as the relevant legal rationale provided by the European Court of Justice (ECJ). It could also prove beneficial to consult the guidelines and opinions of the European Data Protection Board (which comprises representatives from the data protection authorities of EU member states).

3.1. Data protection principles

The LPDP establishes key principles governing the processing of personal data.

These principles include:

- legality,
- fairness and transparency
- limitation of the purpose,
- data minimization,
- data accuracy,
- storage limitation,
- integrity and confidentiality,
- responsibility.[19]

19 LPDP, Article 9.

3.1.1. Legality

The processing of personal data is deemed legal only when conducted on bases explicitly permitted and defined in the slegislation.[20] A thorough examination of each processing basis is presented in the fourth chapter of this guide.

3.1.2. Fairness

Once legality as a principle is met, the focus shifts to ensuring fair, i.e. equitable processing. This implies that the personal data subject must be aware that their data will undergo processing. This empowers the personal data subject to make an informed decision about whether they consent to such processing, enabling them to exercise their rights regarding the protection of their personal data.

3.1.3. Transparency

Closely tied to the principle of fair processing is the principle of transparency, signifying that the controller must be forthright and clear with the data subject regarding the processing of their personal data. Under the new legal regulations, instead of the previous notification to the Personal Data Protection Agency, the controller now bears the responsibility of informing the data subjects of the personal data being processed. This notification must be timely and communicated using clear and simple language.

20 Legality of personal data processing
Article 10
(1) The processing of personal data is lawful only if and to the extent that at least one of the following conditions is met:
– the data subject has consented to the processing of their personal data for one or more specific purposes,
– the processing is necessary to fulfill a contract where the data subject is a contracting party or to undertake activities at the request of the data subject before their accession to the contract,
– the processing is necessary to fulfill a legal obligation of the controller,
– the processing is necessary to protect the vital interests of the data subject or of another natural person,
– the processing is necessary for the performance of tasks carried out in the public interest or in the exercise of official authority vested in the controller by law,
– the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except when such interests are overridden by the interests or fundamental rights and freedoms of the data subject that require the protection of personal data, especially when the data subject is a child.
(2) The provisions of paragraph 1, indent 6 of this article shall not apply to the processing of personal data by state bodies in the exercise of their competences.
(3) The legal basis for the processing of personal data specified in paragraph 1, indent 3 and 5 of this article shall be established by law. The law provides mandatory provisions for: the conditions that determine the legality of the processing by the controller, the purposes of the processing, the categories of personal data that are the subject of the processing, the categories of data subjects; entities to which personal data may be disclosed, as well as the purposes for which personal data is disclosed, limitations regarding processing purposes, storage period, processing operations and procedures, including measures to ensure legal and fair processing, and to fulfill the purpose of the public interest while being proportional to the performance of the legitimate purpose. The law must also include an assessment of the impact on the protection of personal data for the cases provided for in Article 39 of this law.
(4) If personal data are processed for a purpose other than the purpose for which they were originally collected, where the processing is not carried out on the basis of the consent of the data subject or on the basis of a law, which is a necessary and proportionate measure for the protection of the purposes established in Article 27 paragraph 1 of this law, then the controller, in order to determine whether the processing for other purposes is in accordance with the original purpose for which the personal data were collected, is obliged to take into account, among other things:
– any connection between the purposes for which the personal data are collected and the purposes for the intended further processing,
– the context in which the personal data were collected, especially with regard to the relationship between the data subjects and the controller,
– the nature of the personal data, specifically whether special categories of personal data are processed in accordance with Article 13 of this law, or if personal data related to criminal convictions and offenses are processed in accordance with Article 14 of this law, and the potential consequences of the intended subsequent processing for the data subjects.
– the presence of appropriate safeguards, which may include encryption or pseudonymization.

3.1.4. Limitations of the purpose

Purpose limitation implies that controllers can process personal data solely for specific, clear, and legitimate purposes. This implies that controllers must initially identify the specific purpose for which they will process the personal data, and the identified purpose serves as the framework within which the processing will occur. Subsequent (secondary) processing, involving a purpose different from the original one, can be deemed legal only if it is considered compatible with the initial purpose for which the personal data were originally processed.

3.1.5. Minimum data volume

The principle of minimal data processing stipulates that controllers will only process personal data that is adequate, relevant, and limited to what is necessary to achieve the intended purpose. The controller is obligated to ensure that the processing is genuinely necessary and that the amount of personal data processed is proportionate to the intended purpose of the processing.

3.1.6. Accuracy

The principle of accuracy implies that the controller must institute suitable measures for the personal data it processes. The personal data must be accurate and, when necessary, kept up-to-date. The controller is also responsible for implementing measures to promptly delete or correct any personal data that is found to be incorrect or incomplete.

3.1.7. Limitations of storage period

According to this principle, personal data will be retained in a format that allows the identification of the personal data subjects for no longer than is essential to fulfill the purposes for which the processing is conducted. In other words, the processing of personal data will be conducted only for the duration necessary to achieve the intended purpose for which the personal data was processed.

3.1.8. Integrity and confidentiality

Personal data can only be processed in a manner that guarantees an adequate level of security, achieved through the implementation of suitable technical or organizational measures. To safeguard personal data, controllers should establish an information security system, the details of which are elaborated in the seventh chapter of this manual. When evaluating and implementing the information security system, it is common and advisable for the team to consist of both legal and technical professionals to ensure a more comprehensive approach to defining the controller's strategies and policies.

3.1.9. Responsability

Responsibility in the realm of personal data is a mutual obligation. It is incumbent upon everyone to ensure the safeguarding of their personal data, refraining from public exposure or actions that may jeopardize the data. Certainly, anyone who, in any way, processes, stores, and disposes of personal data made available to them based on legally provided grounds and purposes is equally responsible.

04

USE OF PERSONAL DATA FOR LEGAL PURPOSES AND ON THE BASIS OF A LEGAL MATTER

IV.

USE OF PERSONAL DATA FOR LEGAL PURPOSES AND ON THE BASIS OF A LEGAL MATTER

The concept of entrusting personal data—meaning their processing, storage, and disposal for legal purposes—involves obtaining consent from the data subject. In certain cases, consent is not required when there are legally valid and justified reasons and circumstances. Nevertheless, the duty of care remains consistent.

4.1. Consent

Nowadays, with the proliferation of new technologies, nearly every website, app, social network, or other data-sharing platform has its own set of rules that necessitate agreement before use. These rules typically manifest in the form of terms of use, cookie rules, privacy policy, EULA (End User License Agreement), and similar documents. Essentially, consent signifies entering into a contractual relationship, which can be terminated under the conditions stipulated in those rules, or a contract. The principles to be observed when giving consent include the following:

4.1.1. Freely given consent

• It entails the choice for the data subject to decide whether to give consent or not, and the option to withdraw it at any time. In evaluating whether consent is freely given, special consideration should be given to whether the data subject is conditioned by the execution of a contract in which they are a contracting party.

4.1.2. Specific consent

• It implies that the data subject has consented only to the specific processing of their personal data. If the controller engages in the processing of personal data through multiple processes, distinct consent should be obtained for each process individually.

4.1.3. Informed consent

• It implies that the data subject has given consent after being provided with all the details of the processing in a language and form that is comprehensible, enabling them to adequately assess the impact that the processing may have on them.

4.1.4. Unequivocal Consent

• It implies that the statement or affirmative action of the data subject leaves no room for doubt regarding their intention to consent to the processing of their personal data.

4.2. When consent is not required

According to the LPDP, the data subject's consent is not the sole legal basis for data processing.

For instance, data processing may also be grounded in a specific law or legitimate interest pursued by the controller or a third party, unless such interests are outweighed by the fundamental rights and freedoms of the data subject. This provision, or postulate, must be interpreted narrowly, specifically referring to cases where the consent of the data subject would be required.

In practice, this provision applies to cybercrime, such as cases where perpetrators operate under a false profile (using the name of another person), exploit personal data for fraudulent activities, or engage in processing data related to child pornography, or when they publish photographs and other sensitive information about others on the Internet with the intent to harm their dignity and reputation by exposing them to the public.

4.3. Rights of the data subject

The data subject is entitled:

- to be informed about the identity of the controller and their representative in the Republic of North Macedonia;
- to gain access to the personal data collection;
- to be aware of which personal data are stored for them in electronic or paper form;
- to be aware of the purposes of the processing of their personal data;
- to be informed about the users or categories of users of the data;
- not to consent about the use of the data for commercial purposes or their transfer to third parties for such purposes;
- to have access to the data and to correct it.

IV.

For instance:

Facebook utilizes data collected from users of its social network to offer more targeted marketing opportunities for advertisers. Similarly, Google can identify the interests of users or websites visited by analyzing search queries, serving as a commercial basis for targeted advertising. When creating an account with Facebook or Google, users encounter a privacy policy that they agree to before proceeding, by clicking “sign up” or “ok”.

4.4. Principle of proportionality

Proportionality refers to a balance between the means employed and the intended purpose. The principle of proportionality entails establishing a reasonable balance between data processing and the intended purpose. In other words, it means that the processing of data is conducted to the extent necessary to fulfill the intended purpose.

To mitigate the disadvantages and risks associated with the enjoyment of the rights to privacy and data protection, it is necessary for restrictions to incorporate adequate safeguards.

When the right to privacy and data protection, on one hand, conflicts with other human rights, on the other, the principle of proportionality becomes the primary legal tool employed to balance the various human rights. Subsequently, a balancing test should be conducted.

The proportionality test involves three steps: appropriateness (whether the interference is genuinely suitable to achieve the purported aim), necessity (also known as “less restrictive alternative” or “minimum harm”; determining whether the measure taken is the least restrictive alternative), and proportionality in the strict sense (whether the benefits achieved outweigh the limitations imposed). Furthermore, data processing must be grounded in national law and serve a legitimate purpose.

05

CYBERSPACE SECURITY – CYBER SECURITY AND CYBER HYGIENE

V.

CYBERSPACE SECURITY - CYBER SECURITY AND CYBER HYGIENE

Private personal data are available to third parties on social media platforms, in particular, which sometimes are not only published, hence made public for all. Also, they can contain private information, such as personal photos, and information that - in the analog world - would not be easily available. Many data breaches occur in the online environment. Data breaches are performed by persons who misuse the Internet risks, and sometimes, the negligence of Internet users, and process the personal data of the users for their own purposes.

5.1. Three types of cybersecurity

The cybersecurity encompasses a large scope of tools and techniques, as follows:

5.1.1. Data security

Hackers often search for data. They want to look at or steal information that is beyond any boundaries. The reasons for that are various. In some cases, the hacker steals information such as credit card numbers to sell them on the Dark web. In other cases, the purpose is not lucrative, but rather to harm somebody by publishing personal data, or just to obtain the data, in order to satisfy political, business or other appetites. Data security involves protecting data from unauthorized access. It envisages data encryption, data access control technologies and policies.

5.1.2. Network security

For a cyberattack to be successful, in almost any scenario, the hacker must initially gain access to the target's network. Network protection is one of the most serious areas of cybersecurity and it is often the focus of significant investment. Network security is a set of rules and configurations designed to protect the integrity, confidentiality and access of computer networks and data by using software and hardware technologies.

5.1.3. Application security

Hackers also want to enter into software applications like Enterprise Resource Planning (ERP), CRM, email servers and so on. In-app presence is a great way to spy on a target or disrupt one's own operations. Application security has many aspects, but it usually combines the policies (for example, who is allowed to access the application and the administrative "backend") and controls over the application programming interfaces (APIs) that allow other software programs to access to the application.

5.2. Types of threats

The categorization of threats is based on the entities they target, leading to the following divisions:

- Threats to persons
- Threats to property
- System threats

There are seven common types of cybersecurity threats. A cyber threat is a method of attacking data assets. It is not a real attack. It resembles more a plan of attack. There are millions of cyber threats out there. In general, they are the following:

- VIRUSES/MALWARE – A virus is a form of malicious software code that installs itself on your device. Once installed, the virus can perform a variety of malicious activities, such as, freezing the system, stealing data, even hijack devices for illegal purposes, such as mining cryptocurrencies without your permission, for example, "cryptojacking".

- IDENITITY THEFT – Identity theft is a crime where a hacker steals enough of your private, personal information (for example, social security number, date of birth, address, etc.) to impersonate you. By pretending to be you, a hacker may be able to steal money from your bank account, open credit card accounts in your name, and more.

- PASSWORD ATTACKS – If a hacker has your password, he or she can get into your accounts. Password attacks use special software to guess passwords, often trying thousands of possible combinations of characters until the correct password is found.

- „TROJANS“ – Like the famous Trojan Horse of ancient times, a Trojan virus is a cyberattack that infiltrates a target's network under false pretenses. For example, a hacker can embed a virus in a PDF document and send it to you as an email attachment. When you open the PDF document, the file embeds the virus in your system as the document opens in Acrobat Reader.

- RANSOMWARE –It is a type of malicious software that encrypts your data and restricts users' access to it until a ransom, usually in Bitcoin, is paid to unlock it.

PHISHING – An attempt, usually via email, to trick you into clicking on a hyperlink that will install malware on your computer. A more sophisticated form of attack, known as spear phishing, involves the attacker impersonating a friend or colleague, usually with the goal of making you share account login credentials. Phishing is a social engineering technique used to steal data or commit fraud. This is committed by sending fake ads through fake websites to unsuspecting users. Advertisements usually contain sales promotions for various goods, including, for example, accessories or vehicles at attractively low prices. This is done to lure potential victims into sharing sensitive information, such as personal details, usernames and passwords, as well as payment card and bank details.

ADVANCED PERSISTENT THREAT (APT) – APTs are arguably the most powerful cyber threats. APT is designed to sneak in and then lurk in your network for months, undetected. It moves laterally, installing itself over and over again in different parts of your infrastructure until it is activated. Then, it can do incredible damage.

5.3. Cyber hygiene

Cyber hygiene refers to a set of practices and measures you can undertake to maintain your digital security and protect yourself from cyber threats. Just as personal hygiene practices, such as hand washing and brushing teeth help prevent the spread of germs and disease, cyber hygiene practices help prevent the spread of malware, viruses and cyberattacks.

06

DIFFERENT “ACTORS” IN THE FIELD OF PRIVACY AND PERSONAL DATA PROTECTION

VI.

DIFFERENT "ACTORS" IN THE FIELD OF PRIVACY AND PERSONAL DATA PROTECTION

The issue of personal data protection is a complex one. It is a conglomerate of measures, activities, authorities, persons and companies that do not always have clear and delimited boundaries and competences.

6.1. Assembly of the Republic of North Macedonia

The legislature provides the constitutional and legal framework, inter alia, in this area. In the context of this guide, it is crucial to highlight that the notion of an independent supervisory body is implemented within the legal framework of the Republic of North Macedonia (RNM) through the Personal Data Protection Agency. This agency, in turn, is accountable for its operations to the Assembly of the Republic of North Macedonia.[21]

6.2. Personal data protection agency

As an autonomous and independent regulatory body, the independence of this institution is exceptionally clearly and strongly established and affirmed through normative means. The agency is completely politically, financially and functionally independent in the performance of its competences, tasks and powers, and its director, deputy and employees may not receive or seek instructions from state government bodies, municipal bodies, the bodies of the city of Skopje or any other legal and/or natural persons.

This agency performs its supervisory function through supervision, which can be:

- regular supervision,
- extraordinary supervision, and
- control supervision.

Within its competences, the PDPA may initiate misdemeanor proceedings and impose fines on a controller who violates data protection, which is punishable behavior according to the provisions of the LPDP.

21 LPDP, Article 57.

The Agency shall be held accountable for its work before the Assembly of the Republic of North Macedonia, and its decisions shall be controlled by the judiciary, in accordance with the constitutional principle referred to in Article 15 of the Constitution and Article 6 of the ECHR.[22] According to the LPDP, the Agency is not competent to supervise the courts when they act within their judicial functions, except for supervision over the legality of the activities undertaken during the other processing of personal data carried out by the courts in accordance with the law.

6.3. Courts

According to the Constitution, judicial protection against the acts of the state administration and state bodies is guaranteed. The right of access to court under equal conditions for all is also a guaranteed right. In RNM, courts are organized according to the principle of regular courts. Regular courts are structured based on the principle of territorial jurisdiction, primarily categorized into civil and criminal courts on one hand, and administrative courts on the other.

The court in this area plays a double role. The first role is to act as a data controller due to the information it possesses, as judges are not exempt from adhering to data protection laws. For instance, while conducting their proceedings, they should consider the principle of data minimization, meaning they can only collect or process personal data that is essential for the proceedings, and they should appropriately anonymize their judgments. Only personal data that are relevant to solving the case will be processed in the case files. Particular attention must be paid to the extent to which the parties have access to the case files. For example, the suspect must not have access to the personal data of the victim or witnesses, such as the address, telephone number and other data that is sensitive in this regard.

Furthermore, the court acts in a capacity of an actor in the protection of public and private interest in relation to personal data. These capacities will be discussed in more detail below.

22 Constitution of the RNM, Article 15
The right to appeal against individual legal acts issued in a first instance proceedings by a court, administrative body, organization or other institution carrying out public mandates is guaranteed.

6.3.1. Administrative courts

Administrative courts inter alia are responsible for granting judicial protection of the decisions of the Personal Data Protection Agency, that is, they provide legal protection in the field of administrative matters, in connection with the protection of personal data and the application of the LPDP. These courts ensure the principles of constitutionality and legality (in a broader sense, together with the application of international standards).

6.3.2. Civil courts (civil matter)

The issue of personal data protection and human rights, especially in relation to the cyberspace, is not limited to data protection and ensuring that one's data is kept properly. The mishandling, improper storage, or unauthorized disclosure of data can, indeed, lead to a violation of personal rights and, in such cases, individuals have the recourse to seek protection through civil courts for compensation for damages. In such cases, the rule nemo iudex sine actore is applicable, as well as the principle actori uncubit probatio. The first implies that the court doesn't act ex officio but only when summoned to address a significant human rights claim (lawsuit), and it is the responsibility of the plaintiff to demonstrate that the elements of the legal norm to which they refer are satisfied.[23] In such cases, according to the general principles for damage compensation, the plaintiff usually has to prove as follows:

- There is a harmful effect (which can be through active conduct or by omission thereof) and to adequately describe it, that is, to explain it;
- there is an identified perpetrator who is responsible for such action or has not taken surveillance measures to prevent such actions or to remedy the omission by taking action and identifying it;
- There should be evident harm in any of its manifestations, primarily non-material damage resulting from the infringement of personal rights, and it needs to be clearly elucidated, detailing its nature and extent;[24]
- There is a nexus between the harmful effect and the perpetrator;
- The extent of the damage will be appropriately quantified, employing the rules of evidence and utilizing the available proof;
- If the damage cannot be quantified, that is, its quantification would cause significant difficulties, then the Court can decide based on a free assessment.[25]

23 Grounds of responsibility
Article 141
(1) Whoever causes damage to another through fault, is obliged to compensate it.
(2) For damage caused by objects or activities that result in an increased risk of damage to the environment, liability is held regardless of fault.
(3) Damage regardless of fault is also liable in other cases provided for by law.
Damage
Article 142
Damage is the decrease of one's property (casual damage) and the prevention of its increase (lost benefit), as well as the violation of personal rights (immaterial damage).
Request to remove the danger of damage
Article 143
(1) Anyone can ask another person to give up the source of danger that threatens him/her or an indefinite number of people with significant damage, as well as to refrain from an activity from which a disturbance or danger of damage arises, if the occurrence of the disturbance or the damage cannot be prevented by appropriate measures.
(2) The court, at the request of the interested person, shall order appropriate measures to be taken to prevent the occurrence of damage or disturbance or to remove the source of the danger, at the expense of the owner of the source of the danger, if they fail to do so by themselves.
(3) If the damage occurs in the performance of a public benefit activity for which a permit has been obtained from the competent authority, only compensation for the damage that exceeds the normal limits (excessive damage) can be requested.
(4) In the case referred to in paragraph 3 of this article, it may be required to take socially justified measures to prevent the occurrence of damage or to reduce it.
Request to cease violation of personal rights
Article 144
(1) Every person shall be entitled to ask a court or other competent authority to order the cessation of an action that violates their personal right and to order the removal of the consequences caused by this action.

24 How immaterial damage is compensated
Article 187-a
Immaterial damage is compensated immaterially (moral satisfaction) and materially (material satisfaction) in the cases provided for in law.
Publication of judgment or correction
Article 188
In the case of a violation of personal rights, the aggrieved party has the right to request, and the court may order, at the expense of the wrongdoer, the publication of the judgment, which involves correcting or retracting the statement that caused the violation, or any other measure that can contribute to achieving the objective pursued by the fair monetary compensation.
Fair monetary compensation
Article 189
(1) In the event of a violation of personal rights, the court, if it finds that the severity of the violation and the circumstances of the case justify it, shall award a fair monetary compensation, regardless of the compensation for material damage, as well as in the absence thereof.
(2) When deciding on the request for fair monetary compensation, the court shall take into account the severity and duration of the injury that caused physical pain, mental pain and fear, as well as the purpose for which the compensation serves, but also that the compensation should not be contrary to aspirations that are incompatible with its nature and social purpose.
(3) In the event of a violation of the right to reputation and other personal rights, the court, if it finds that the severity of the violation and the circumstances of the case justify it, shall award a fair monetary compensation, regardless of the compensation for material damage, as well as in the absence thereof.
(4) In addition to these rules, in certain cases, when it is regulated differently by another law, the rules of that law shall also be applied.

25 Law on Civil Procedure
Article 209
If it is established that the party is entitled to compensation for damages, a monetary amount or replaceable objects, but the amount of the amount, that is, the quantity of the objects cannot be determined or could only be determined with disproportionate difficulties, the court shall decide based on free assessment.

6.3.3. Damage compensation according to the LPDP

Interestingly, the LPDP contains provisions for damage compensation that are lex specialis. According to the principle of lex specialis derogit legi generali[26], at first glance it seems that these provisions replace the general provisions and principles for compensation of damage. However, the provision stated in the LPDP refers to the violation of the provisions of this law.[27]

26 VIII JUDICIAL REMEDY AND LIABILITY
Right to file request to the Agency
Article 97
(1) Every data subject shall have the right to file a request with the Agency if the data subject considers that the processing of personal data relating to him or her infringes provisions of this Law, without prejudice to any other administrative or judicial remedy.
(2) The Agency shall inform the complaining party of the progress and outcome of the procedure, including the possibility of a judicial remedy pursuant to Article 98 of this Law.
(3) The form and content of the request template referred to in paragraph (1) of this Article shall be prescribed by the director of the Agency.
(4) The Agency shall decide whether to reveal, during the procedure, personal data of the complaining party, to the contesting party as well as to the witness.
(5) The Agency shall initiate supervision in accordance with provisions of this Law for the filed request referred to in paragraph (1) of this Article.
Right to effective judicial remedy against decisions of the Agency
Article 98
(1) Each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them, without prejudice to any other administrative or non-judicial remedy.
(2) Without prejudice to any other administrative or non-judicial remedy, every data subject has the right to effective judicial protection, when the Agency in accordance with the competencies determined in Articles 65 and 66 of this Law has not acted upon the request or has not informed the personal data subject within three months for the outcome of the procedure upon the submitted request according to Article 97 of this Law.
Right to an effective judicial remedy against a controller or processor
Article 99
(1) Without prejudice to any available administrative or non-judicial remedy, including the right to submit a request to the Agency in accordance with Article 97 of this Law, every data subject shall have the right to effective judicial protection when it considers that his/her rights determined by this Law have been violated, as a result of the processing of his/her personal data contrary to this Law.
(2) The data subject shall exercise its right referred to in paragraph (1) of this Article by filing a lawsuit to the competent court in accordance with law.
Representation of data subjects
Article 100
(1) The data subject shall have the right to mandate a citizen association to lodge the request on his or her behalf in relation to personal data protection, in order to exercise the rights referred to in Articles 97, 98 and 99 of this Law, and, if provided for by law, to exercise the right to compensation referred to in Article 101 of this Law.
(2) The statute of the citizen association referred to in paragraph (1) of this Article established in accordance with law, shall mandatorily indicate their goals which serve the public interest, its nonprofit character, as well as that the association is active in the field of data protection and protection of the rights and freedoms of data subjects.
Right to compensation and liability
Article 101
(1) Any person who has suffered material or immaterial damage as a result of an infringement of this Law shall be entitled to compensation from the controller or processor for the damage suffered.
(2) Any controller involved in the data processing shall be liable for the damage caused by processing which infringes this Law. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Law specifically directed to processors or where it has acted beyond or contrary to lawful instructions of the controller.
(3) A controller or processor shall be exempt from liability under paragraph (2) of this Article if they prove that they are not in any way responsible for the event giving rise to the damage.
4) Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are, under paragraphs (2) and (3) of this Law, responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject (joint liability).
(5) Where a controller or processor has, in accordance with paragraph (4) of this Article, paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage, in accordance with the conditions stipulated by paragraph (2) of this Article.
(6) Court proceedings for exercising the right to receive compensation shall be brought before a competent court in accordance with the law.

27 LPDP, Article 101.

6.3.4. Criminal courts (criminal matter)

Similar to the civil courts, criminal courts also administer justice and adjudicate cases that touch on the subject matter covered in the present guide. They, also, apply the nemo iudex sine actore principle, as well as the actori incubit probatio principle. A difference is that in criminal proceedings, the presumption of innocence is an imperative principle that prevails above all.

Criminal courts are not only actors when adjudicating cases that use a protected social good - personal data and human rights, but at the same time they are also guarantors of those rights, in regard to all participants, and especially to persons who are suspected or accused of crimes. Primarily, this pertains to the role of criminal courts in the domain of special investigative measures, encompassing their authorization, duration, presentation, storage, and eventual destruction.

However, when discussing courts adjudicating individual criminal offenses in contrast to the Law on the Personal Data Protection (LPDP), in practice, there is a notable overlap of elements delineating what constitutes a criminal offense according to the provisions of the Law on the Personal Data Protection and the Criminal Code.

If the misdemeanor provisions in the LPDP are analyzed, each violation refers to a specific provision of the law and acting contrary to that provision entails criminal liability.

The criminal offense that is closest to the topic covered by this guide is Abuse of personal data, according to Article 149 of the Criminal Code.[28] The essence of such offense prefers to possess the following in its basic form:

- Illegal behavior which is per se against the law! (Although the initial association may be that for the LPDP, there could be provisions for the handling of personal data in other laws, extending beyond the scope of the LPDP alone.)
- Actus reus is the collection, processing or use of personal data.
- Such an action is done without the consent of the person whose data has been abused.

Effects of committing the offenses are described in more detail in the misdemeanor provisions of the LPDP. The criminal offense, however, as prescribed, has a relatively broad scope. The answer to the question what constitutes a difference between a misdemeanor and a criminal offense, when the act of committing it is relatively the same, may be found in the fact that in the case of a criminal offense, at least in its basic

28 Abuse of personal data
Article 149
(1) Whosoever, contrary to the conditions determined in line with a law, and without the consent of the citizen collects, processes or uses their personal data shall be fined or sentenced to imprisonment of up to one year.
(2) The sentence referred to in paragraph 1 shall be imposed to a person who shall brake in a computer information system of personal data, with the intention to use them for personal or benefit for another, or to cause damage to another.
(3) If the crime referred to in paragraphs 1 and 2 is committed by an official person while performing the duty, that person shall be sentenced to imprisonment of three months to three years.
(4) Any attempt shall be punishable.
(5) If the crime stipulated in the present Article is performed by a legal person, it shall be sentenced with a fine.

form, there is no data collection, while in the case of misdemeanors, they refer to a data collection. However, a general and universal rule cannot exist and each case must be evaluated individually, with all the facts and circumstances surrounding it.

Criminal courts, that is, proceedings, are called to act not only in this criminal offense, but also in case of other offense that aim at illegal use of personal data. Thus, a multitude of criminal acts, more or less, refer to personal data, and these are some of them:

- Unauthorized publication of personal notes – Article 148;
- Unauthorized disclosure of a secret – Article 150;
- Unauthorized tapping and audio recording – Article 151;
- Unauthorized recording – Article 152;
- Production and distribution of children pornography – Article 193-a;
- Damage and unauthorized entry into a computer system – Article 251;
- Creating and spreading computer viruses – Article 251-a;
- Computer fraud – Article 251-b;
- Computer forgery – Article 379-a;
- Terrorism – Article 394-b;
- Spreading racist and xenophobic material via information system – Article 394-d;
- Extortion – Article 258;
- Blackmail – Article 259.

However, criminal courts are not only called upon to adjudicate, but also have an obligation to preserve data obtained by special investigative measures, certain evidence, especially electronic/digital evidence, DNA material, biological material, etc.

6.4. Public prosecutor's office

The Public Prosecutor's Office is part of the judicial apparatus of a country, and it is one of the necessary links. Structured based on the principles of hierarchy, legality, limited authority, the Public Prosecutor's Office (PPO) is tasked with prosecuting perpetrators of crimes related to data protection and human rights in cyberspace. Recently, the Public Prosecutor's Office has been facing a serious influx of new generation crimes, driven and led by new technologies, for example, hate speech on social networks and the similar acts. Each case is examined individually whether it constitutes a more benign speech, that is, an expression, as opposed to a harsher one, which contains the elements of a crime. In fact, the subsumption of the legal norm can only be carried out after a complete clarification of the facts and circumstances, that is, after a complete and thorough investigation.

In the context of the message, there are instances where evidence and/or information is sourced from the so-called VASP (Virtual Assets Service Provider), which refers to service providers dealing with virtual assets (Bitcoin, FTH, Litecoin, etc.). Currently, there is only one such provider in the Republic of North Macedonia.

A common scenario in practice involves the deception of individuals interested in trading or purchasing virtual assets (cryptocurrencies) and they provide their personal data to these providers, some of which are legally registered in certain jurisdictions, while others operate without proper legal authorization. Interestingly, even if these entities are physically situated in one territory, the data or records they handle are often located abroad, stored on servers in different jurisdictions, such as in virtual banks, and so forth.

Again, all abuses of personal data, that is, privacy, are assessed and evaluated on a case-by-case basis, based on all the facts and collected evidence.

In order to establish reasonable suspicion, and subsequently a well-founded suspicion that a criminal offense, typically under Article 149 of the Criminal Code, has been committed, there must be a minimum level of threat. This threat extends beyond the mere acquisition or taking of data, and encompasses the potential misuse of the data in a manner contrary to the law.

However, this criminal offense is not always the one that contains all the elements, because the purpose of the one who abuses them is to use them for his own illegal gain or for another illicit purpose. Hence, it is not uncommon for personal data to be acquired with the intention of securing fast loans, exploiting other associated rights (such as social or pension benefits), or engaging in activities like insurance fraud, and so forth. All these situations contain similar facts, but the final product, from the point of view of subsumed legal norm does not have to be only the criminal offense as referred to in Article 149, but also as a result of that abuse of data, there can be one or more criminal offenses. Regardless whether it is in real or ideal stack.

6.4.1. Chain of Custody

In such cases, ensuring the integrity of the evidence, specifically the data acquired during the investigation, becomes exceptionally important. If the evidence does not have a clear movement through the chain of persons and bodies it passes through, its security is not guaranteed, not only in physical sense, but also in terms of not being subject to alteration or modification, because their evidentiary value might be compromised.

From a practical point of view, it should be noted that these cases, by definition, require the involvement of technical experts/professionals in order to extract the data needed in the proceedings. It should be explicitly emphasized here that the responsibility of technical experts is to explain the content of the data, which involves detailing its location, ownership, and accountability (including metadata, who is the creator, collector, medium, modification history), but their role does not extend to providing testimony or offering opinions about the data. The ultimate goal is to create, that is, to prove, a connection between the data and the suspect. Certainly, in order to satisfy the interests of a fair proceedings, the defense will have the right to cross-examine this person.

6.5. Advocacy

The legal profession - advocacy, as an integral component of the judiciary, holds a highly specific role in this domain. On one hand, there is a legal and ethical obligation, as outlined in acts and the code of the bar association, to retain and process personal data for one's own clients, and, on the other hand, there is a corresponding obligation to safeguard these data, even when they are crucial to a specific legal proceeding. Primarily, this pertains to the duty to maintain attorney-client privilege, that is, to keep a lawyer's confidence, encompassing information entrusted to or acquired by the lawyer in the course of their work, as well as the right of the lawyer to abstain from testifying about information acquired during their work and the relationship with their client.

On the other hand, the advocacy is a public profession and therefore it collects data for which it is also responsible, like all other entities. Particularly today, in the digital age, when data increasingly come in digital form. As the lawyer's communication with its clients and with the authorities grows, so do the obligations. This implies that lawyers do not have immunity when it comes to personal data and the aspect of human rights in cyberspace, but they have a positive obligation to protect and indicate any possibility of abuses.

One of the paramount obligations of the legal profession is to thoroughly comprehend the intricacies of new technologies and their normative aspects in order to identify potential risks and abuses associated with these technologies, facilitating the provision of timely, precise, and effective legal advice. Furthermore, adhering to these principles allows legal professionals to effectively exercise procedural and substantive powers when assuming roles such as procedural assistants, attorneys, and defense attorneys in various proceedings (including civil, administrative, criminal, misdemeanor, and others).

During the proceedings, the legal professionals have the opportunity to obtain findings and opinions from experts and technical advisors just like the prosecutor in the criminal proceedings and under equal conditions with the opposite party. Postulates that apply in these conditions have been discussed in the above section referring to the public prosecutors.

6.6. Police

When discussing the police, the immediate association is, of course, their role in terms of the subject matter of this guide, which involves the detection of criminal acts and offenses. According to the arrangement of the criminal and legal system in RNM, there are two types of investigations, that is, preliminary investigations, which are undertaken by police officers. These are reactive and proactive investigation. The postulates and examples that apply to the actions of the public prosecutor's office also apply to the police, that is, to the judicial police.

Regarding personal data, the police must adapt accordingly to the development of society and the emergence of new forms of crime.

Criminal acts committed through computer systems and/or the Internet, with the objective of infringing upon the right to privacy as a fundamental human right and violating personal data, can be categorized in four ways:

1. These are illegal actions that represent a violation of important individual and social goods for which the law provides criminal sanctions.
2. They were committed in a specific way, with the use of specific means and purpose of the crime - and that is with the use of computer systems and networks.
3. These acts fall under a distinct category of protection, focusing, for instance, on the security of computer systems and networks, as well as streaming of stored computer data, either in its entirety or in specific parts.
4. The purpose of the perpetrator of these acts is to obtain an illegal benefit (material or immaterial) or to cause harm to others.[29]

However, the police cannot be seen as an isolated entity in the fight against crime, as violations of the law do not always equate to crimes and vice versa. The scope of regulation that dictates personal data and its protection doesn't always fall within the jurisdiction of the police. Thus, for example, when it comes to the misuse of personal data, the police establish jurisdiction here, because there is probably grounds for suspicion of a criminal offense. On the other side, when it comes to the illicit handling of the personal data collection, even if the same set of facts might prima facie raise suspicion of both a criminal offense and a regulatory offense under the LPDP, the latter may take precedence, because there is a personal data collection, and there could be irregularities in the management of personal data collection without constituting a criminal act.

29 I. Marcella, Albert J. II. Greenfield, Robert, Cyber Forensics, CRC Press, 2005, p. 48.

VI.

If

crime = act (or omission) + **illegality** + **punishability** +

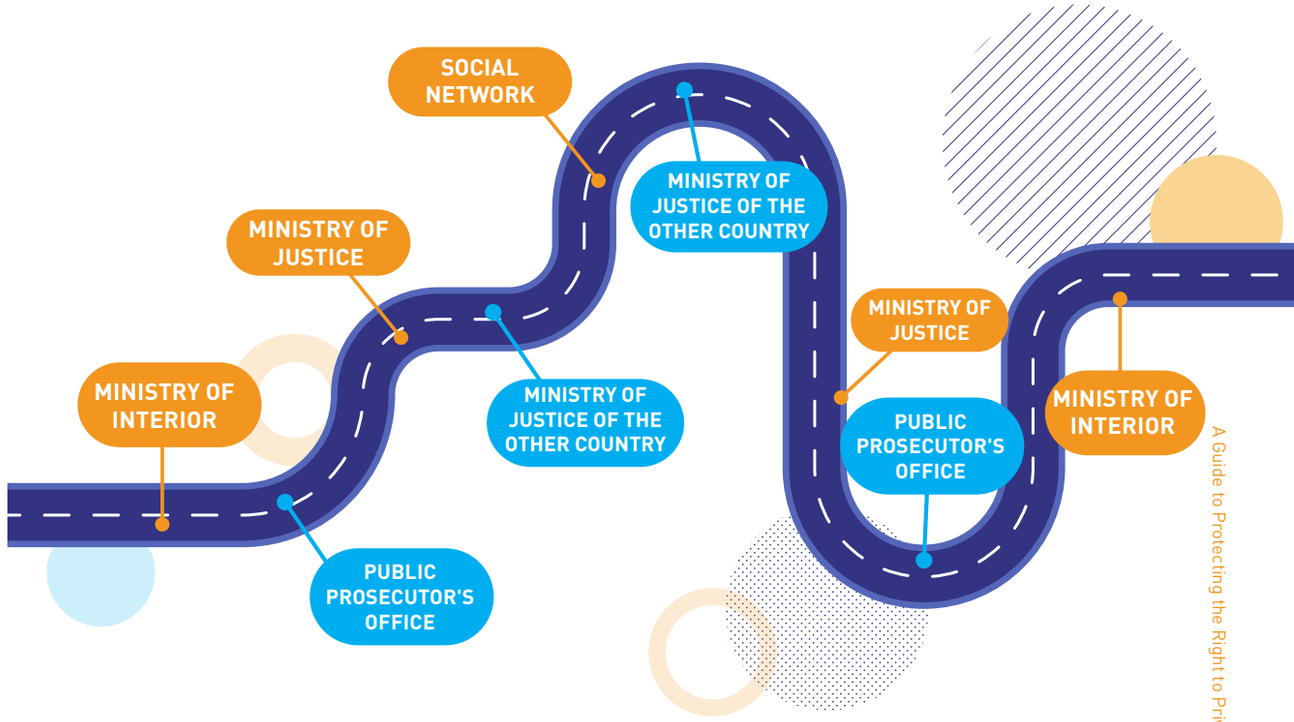
volitional attitude towards the crime (intention/negligence)

Then the absence of any of these elements means that there is no crime. But that does not exclude the existence of another delict.

Thus, for example, the PDPA has jurisdiction over the removal of fake profiles on social networks, while the police would have jurisdiction over the consequence that arose as a result of that created fake profile (damage, fraud, extortion, etc.), because it is a prescribed criminal offense under CC.

A distinct category of procedures involves requests for international legal assistance, which are quite common, given the circumstances that personal data on the Internet is not confined to the territory of a single country. On the contrary, they can be situated not only in a foreign country but also in multiple jurisdictions. Last, but not least, the entities that operate such systems often cannot be identified, which means that international legal assistance must be requested. Although we live in a society where communication is mostly done electronically, these procedures are still strictly in written form, involve many institutions and there is a lot of waiting for feedback.

The path of that international legal assistance is as follows:



6.7. State bodies

State authorities also play an important role. They primarily function as controllers of personal data and manage collections of personal data that may warrant the highest degree of protection. Protection may be sought in administrative proceedings, specifically concerning the rights of data subjects (such as the right of access, rectification, erasure, and objection) or the determination of the illegality of data processing (when it deviates from the principles of data protection and/or other provisions governing the legality of data processing).

6.8. Civil society organizations

Civil society organizations have an outstanding role in building democratic institutions and developing awareness of the importance of protecting human rights, including those in the cyberspace. Civil society organizations often play a pivotal role in raising awareness within society and establishing protective mechanisms through various means such as trainings, campaigns, strategic representations, and active participation in the development of clear policies.

VI.

6.9. Companies

In the course of their daily operations, companies collect and process personal data and thus they have the role of controllers. Their obligation is twofold, extending both towards the regulator, that is, to be in compliance with regulatory requirements and legislation for data protection, and towards the individuals whose data they store and process—this includes both their employees and third parties who are not in an employment relationship but whose data they access.

The big international conglomerates, that is, the multinational companies that collect data within their competences, or the services and products they offer, must be mentioned here. These include the inevitable social networks (Facebook, Instagram, X, LinkedIn, etc.) and Internet service providers (Google, Yahoo, etc.).

6.10. Individuals

One of the basic rules of data protection is, in fact, that it is the primary obligation of the individual. Everyone has the right to privacy, but also the obligation to diligently take care of the security of their own data. In more recent times, with technological advancements, it is natural persons who, either by their own actions or due to a lack of proper supervision, disclose their own data, thereby exposing themselves to potential risks. Indeed, glaring examples include actions like sharing PIN codes for payment cards, neglecting to verify the security of websites before leaving account details, freely sharing medical data across various platforms, and opening suspicious emails that may attempt to install malicious software, among others. Hence, individuals are not solely victims but also active participants in the realm of data protection, as self-protection is consistently the most effective form of protection.

07

PERSONAL DATA, HUMAN RIGHTS AND THE ISSUE OF ARBITRABILITY

VII.

PERSONAL DATA, HUMAN RIGHTS AND THE ISSUE OF ARBITRABILITY

The implementation of the General Data Protection Regulation from 25 May 2018 caused a far reaching reaction, which did not avoid the arbitration community.

In a few words, the question at hand is whether personal data is a field of law subject to arbitration, i.e. it may be put under one of the regimes for alternative dispute resolution (arbitration), domestic or international. Applying Personal Data Protection law during arbitration procedures may really be very complex (and potentially burdensome), and may impose additional obligations to the parties (arbitration institutions) involved in the procedure, which should be taken very seriously considering the liability risks arising from GDPR.

Despite the importance of application of GDPR in international arbitration, there is a prevalent opinion that it would be unfortunate to think that the new legal regimes which regulate and protect data (such as the GDPR) were only a source of worry for the global arbitration community. On contrary, these legal regimes, which create new legal obligations, will probably generate new legal challenges and legal disputes, which would again, in particular circumstances, be put forward to arbitration and other alternative dispute resolution mechanisms. Consequently, it is not surprising that providers appeared of arbitration and other services for alternative dispute resolution (ADR) so as to offer tools for resolution of disputes online connected with GDPR (particularly for data violation disputes). In any event, it is clear that in our data-driven economy in which data is and will be a key driver of innovation and power, the volume and strategic importance of "data disputes," generally defined as disputes relating to the conditions of protection, of access to and/or of use of data in certain circumstances will (continue to) increase significantly in the future.[30]

30 Using arbitration and adr for disputes about personal and non-personal data: what lessons from recent developments in Europe? – ARIA – Vol. 30, No. 2, Jacques de Werra, March, 2020.

7.1. The responsibility for protection of privacy and personal data within the domestic and international legal order

In the domestic legal order, the responsibility lies with the controller or processor or other legal or physical entity who has committed any breach of privacy. In other words, if a particular physical entity commits a breach within the domain of the criminal law to another legal or physical entity, it corresponds sui generis in the domestic legal order. Clearly, the State may be the perpetrator of any breach (active or passive action). Within the domestic legal order, the position of the State is equal to a party along with other parties involved.

In the international legal order, the State always has legal subjectivity.

Why are we opening this topic in this Guide?

Usually, national institutions, when they decide within their competences, they respect the standards of the domestic legal order when they perform their constitutional and legal duties, without taking into consideration international standards adopted by the State and transposed in the national system.

In the twentieth century, especially in the twenty first century, the greatest challenge for every legal order is to understand that, although countries are sovereign and independent, yet, the legal order which has adopted international norms is not exclusively theirs, but a part of a greater and broader international legal order. Certainly, with the current level of development of the law, it is a civilization advantage and symbol of every democratic society.

National authorities deciding within the national legal order of the Republic of North Macedonia are obliged, and not opting, the implementation of international standards, i.e. regulations. Such obligation not only arises from the Constitution, but from the numerous other regulations, such as the Law on courts, the Law on civil liability for insult or libel, etc.

This principle may be best illustrated with the following: States may be held responsible for their actions or omissions, failures to abide by the internationally adopted obligations, etc. Yet, things are more complex when we talk about understanding the sources of this doctrine, when the issue is daily functions of any administrative or judicial body in the Republic of North Macedonia, although certain laws are clearly directed to foreign judgements, how to apply them directly, along with the opinions and rationale thereof.

International documents and conventions prescribe the minimum standards of treatment and procedures when speaking of the norms prescribed by such acts. There are different international instruments which prescribe rules which need to be reviewed, interpreted and applied within the national law.

VII.

International standards are applicable for different reasons:

- First, every law or body of laws cannot be seen or interpreted isolated within the domestic legal order, let alone in the international legal order.
- Second, every country which opts to ratify or adopt a particular international legal instrument, shall be obliged to abide to the principles of such international instrument and adequately harmonize its legislation and/or its practice.
- Third, this is required by the basic rules of international law pursuant to the responsibility of the countries for their wrongful acts. The emphasis is on the secondary rules for the State's liability, i.e. the general conditions of the international law by which the State is considered liable for wrongful acts or omissions and the legal consequences arising therefrom. "The draft-articles on the responsibilities of the States for internationally wrongful acts with commentaries" (draft-articles)[31] practically codify the international case law and hence are obligatory for all states.

According to Article 1, "Every internationally wrongful act of a State entails the international responsibility of that State". Among other things, the commentary states the basic principle underlying the articles as a whole, which is that a breach of international law by a State entails its international responsibility.

An internationally wrongful act of a State may consist of one or more actions or omissions or a combination of both. Whether there has been an internationally wrongful act depends, first, on the requirements of the obligation, which is said to have been breached, and, secondly, on the framework conditions for such an act, which are set out in Part One. The term "international responsibility" covers the new legal relations which arise under international law by reason of the internationally wrongful act of a State. The content of these new legal relations is specified in Part Two.

According to Article 2, there is an internationally wrongful act of a State when conduct consisting of an action or omission:

(a) is attributable to the State under international law; and
(b) Constitutes a breach of an international obliga¬tion of the State.[32]

One of the most important articles that differentiates the characterization of such act and its interrelation with the domestic law is Article 3. The article states that "the characterization of an act of a State as inter¬nationally wrongful is governed by international law. Such characterization is not affected by the character¬ization of the same act as lawful by internal law".[33]

In the ELSI case, a Cham¬ber of the Court emphasized this rule, stating that:

Compliance with municipal law and compliance with the provisions of a treaty are different questions. What is a breach of treaty may be lawful in the municipal law and what is unlawful in the municipal law may be wholly innocent of violation of a treaty provision.

Very often, domestic authorities (rightfully so) considered that their procedures and/or omissions or application/interpretation of the law in a particular situation should be viewed from the perspective of the domestic legal order. And when they stand the test of legal remedies, which makes them lawful, i.e. not wrongful.

However, due to absence of any doubt, this text intends to erase all interpretations on the relationship between how one looks at an act from the perspective of domestic and international law, and which perspective is relevant, from the perspective of international law.

Article 4 applies to the conduct of the organs of a State, and according to this article,

1. The conduct of any State organ shall be con¬sidered an act of that State under international law, whether the organ exercises legislative, executive, judi¬cial or any other functions, whatever position it holds in the organization of the State, and whatever its char¬acter as an organ of the central Government or of a territorial unit of the State.

2. An organ includes any person or entity which has that status in accordance with the internal law of the State.[34]

Which means that the principle of attribution applies to all organs, including courts.

In summary, it means that if an act, procedure or similar may be completely legal from the point of the domestic law, the same act, procedure may be completely opposite to the international law.

31 „Draft-articles on the responsibilities of the States for internationally wrongful acts with commentaries", 2001, UN International law commission.

32 „draft-articles for the responsibilities of States for internationally wrongful acts with commentaries", 2001, UN International law commission.

33 Regarding the first of these elements, maybe the clearest court ruling is the one of RSC in the treatment of Polish citizens (Treatment of Polish Nationals and Other Persons of Polish Origin or Speech in the Danzig Territory, Advisory Opinion, 1932, P.C.I.J., Series A/B, No. 44, p. 4.) The Court deprived the Polish Government of the right to file questions to the bodies of the League of nations regarding the application of particular provisions from the Constitution of the Free City of Danzig, with explanation that: according to the generally accepted principles, the State may lean on, in the argument against another State, on the provisions from the Constitution of that other State, however only within the international law and international obligations which have been adopted (...) [C] and contrary to this, a State cannot argue against another State, which in its Constitution has provisions intended for avoiding the obligations imposed by the international law or applicable agreements (...) The application of the Constitution for Danzig may(...) result in infringement of the international obligation (...) regardless whether it is according to the agreements or according to the general international law (...) Yet, in cases of such nature, it is not the Constitution, or other regulations as such, but the international obligations which call for the responsibility of the Free City.

34 „Draft-Articles" for the responsibilities of the States for internationally wrongful acts with commentaries", 2001, UN International law commission. Cited also in Judicial supervision in cases of deprivation of liberty of asylum seekers and the responsibility on the state to adhere to international legal standards. Aleksandar Godzo, Ana Dangova Hug, Dime Gjorchevski, 2021.

For us and for this analysis it is important that this position has been constructed during the decades and for cases that are prominent even today, and represent a source of legal argument and law.

National authorities, especially courts, referring only to national law, and practically ignoring international law, do not question individual lawfulness in the broadest sense of any case, they simultaneously confer responsibility of the State whose organs they are, not only in domestic but also in international frames.

Thus, what is lawful within the national law, does not always mean that is in line with the international law.

In context of the matter described by this Guide, especially when the State is one of the actors in the field of privacy and personal data protection, it is imperative to apply international standards, regardless of the regulation in the national legal order, which may regulate matters or issues differently.

7.2. Data protection and freedom of expression

Data protection and freedom of expression are the two fundamental rights which need to exist in balance. Therefore, it is of crucial importance to legally regulate the criteria which balance the right to personal data protection with the freedom of expression and information. ECHR has developed many criteria, which should be taken into consideration, which have also been reflected in some national laws. According to the Law on personal data protection, this process pays special attention to:

- The nature of personal data,
- The circumstances in which data are obtained,
- The effects of published information on the discussion about public interest,
- How known is the physical person in question and the subject of the information,
- The previous conduct of the relevant physical person,
- Previous consent from the concerned physical person,
- The content, form and consequences from the publication of the information.
- The right to expression also encompasses the right to information.[35]

35 LPDP, Article 81, paragraph 4.

7.3. Protection of the right to privacy and personal data protection through the relevant sentences from ECHR and ECJ

The case law of ECHR follows the technological development of humanity quite well, at least in the case of the Council of Europe, where it belongs.

For better overview, the case law has been compiled in titles, i.e. key words.[36]

7.3.1. The term "personal data" and its scope

In its judgements the Court explains the concept of "personal data" by referral to the Convention of the Council of Europe No. 108 for the protection of individuals with regard to automatic processing of personal data of 28 January 1981, which entered into force in 1985 and was updated in 2018 ("Convention 108"), whose purpose is "to secure in the territory of each Party for every individual (...) respect for his rights and fundamental freedoms, and in particular, his right to privacy, with regard to automatic processing of personal data relating to him" (Article 1) [Amann v. Switzerland (GC), 2000, § 65 Haralambie v. Romania, 2009 § 77]. The Court has clearly indicated that, under Article 2 of Convention 108, the concept of personal data is defined as "any information relating to an identified or identifiable individual" [Amann v. Switzerland (GC), 2000, § 65; Haralambie v. Romania, 2009, § 77].

7.3.2. What do they cover

Such data cover not only information directly identifying an individual (the "data subject"), such as surname and forename [Guillot v. France, 1996, §§ 21-22; Mentzen v. Latvia (dec.), 2004; Güzel Erdagöz v Turkey, 2008, § 43; Garnaga v Ukraine, 2013, § 36, but also any element indirectly identifying a person such as a dynamic IP (Internet Protocol) address; Benedik v. Slovenia, 2018, §§ 107-108].

7.3.3. Legal entities and personal data

Even though the question of personal data protection seems mainly to concern individuals, as regards their Article 8 right to respect for their private life, legal entities are also entitled to rely on this right before the Court if they are directly affected by a measure which breaches their right to respect for their "correspondence" or "home". This was the case, for example, where a company had been ordered to provide a copy of all data on a server shared with other companies (Bernh Larsen Holding AS and Others v. Norway, 2013, § 106) or where the Ministry of Defense, under a warrant, had intercepted the communications of civil liberties NGOs (Liberty and Others v. the United Kingdom,

36 Guide on the case law of the Convention – Data Protection, European Court of Human Rights, 12/98. Last update: 31.08.2022.

2008, §§ 56-57). However, in a case concerning measures involving the protection of personal data of members of a religious organization and respect for their "private life", the organization was not directly affected, and was thus not a "victim" within the meaning of Article 34 of the Convention (Avilkina and Others v. Russia, 2013, § 59).

7.3.4. Forms of personal data

Personal data can take very different forms. For example:

- Internet subscriber information associated with specific dynamic IP addresses assigned at certain times (Benedik v. Slovenia, 2018, §§ 108-109].
- Recordings taken for use as voice samples, being of a permanent nature and subject to a process of analysis directly relevant to identifying a person in the context of other personal data (P. G. and J. H. v the United Kingdom, 2001, § 59).
- Cellular samples and DNA profiles [S. and Marper v. the United Kingdom (GC), 2008, §§ 70-77] or finger prints (ibid., § 84) which, notwithstanding their objective and irrefutable character, contained unique information on the individual concerned and allowed his/her precise identification in a wide range of circumstances (ibid., § 85).
- Information on a given individual obtained from banking documents, whether involving sensitive details or professional activity (M. N. and others v. San Marino, 2015, §§ 51 et seq).
- Data on the occupation of an identified or identifiable individual collected and stored by the police (Khelili v. Switzerland, 2011, § 56).
- Data on Internet and messaging (Yahoo) usage by an employee in the workplace, obtained through surveillance [Bărbulescu v. Romania (GC), 2017, §§ 18, 74-81].
- A copy of electronic data seized in a law firm, even though it had not been deciphered, transcribed or officially attributed to their owners (Kirdök and Others v. Turkey, 2019, § 36).
- Data collected in the context of non-covert video surveillance in a university (Antovic and Mirkovic v. Montenegro, 2017, §§ 44-45).
- Information on the taxable income and assets of a large number of individuals, notwithstanding the fact that the public could access such data under certain conditions [Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland (GC), 2017, § 138].
- Data on the birth and abandonment of an individual, including information needed to discover the truth about an important aspect of personal identity (Gaskin v. the United Kingdom, 1989, § 39; Mikulic v. Croatia, 2002, §§ 54-64; Odievre v. France [GC], 2003, §§ 28-29).
- Data included in a divorce settlement, comprising details as to the division of matrimonial assets, the custody and residence of minor children, the alimony agreement and an overview of the assets/income of the applicant (Liebscher v. Austria, 2021, §§ 31 and 68).

7.3.5. Special categories of data

7.3.5.1. So called "sensitive" categories

Under Article 6 of Convention 108, personal data revealing racial origin, political opinions, religious or other beliefs, and information on an individual's health or sex life, or on any criminal convictions, cannot be automatically processed unless domestic law provides for appropriate safeguards. Information falling within these categories, described by the Court as "sensitive", warrant a heightened degree of protection in its view.

7.3.5.2. Data revealing racial or ethnic origin

An individual's ethnic identity must be regarded as an important element of private life (S. and Marper v. the United Kingdom, [GC], 2008, § 66; Ciubotaru v. Moldova, 2010, § 49). Data is of particular concern where they might reveal a person's ethnic or other origin, bearing in mind the rapid pace of developments in the field of genetics and information technology (S. and Marper v. the United Kingdom [GC], 2008, § 71). Samples and DNA profiles contain much sensitive information and allow the authorities to establish genetic relationships between individuals and assess their likely ethnic origin (ibid., §§ 72-77; Aycaguer v. France, 2017, § 33). In a case concerning the recording of an individual's ethnic origin on the official registers, the Court, emphasizing the highly sensitive nature of the recording of such data, acknowledged the existence of a positive obligation on the part of the State to put in place a procedure to enable the data subject to have his/her recorded ethnicity changed on the basis of objectively verifiable evidence (Ciubotaru v. Moldova, 2010, §§ 52-59).

7.3.5.3. Data revealing political opinions, and religious or other beliefs, including philosophical

Data revealing political opinions are regarded as a "sensitive" category of personal data and, in the Court's view, it is unacceptable for the national authorities to disregard this aspect by processing such data in accordance with ordinary domestic rules, without taking account of the need for protection (Catt v. the United Kingdom, 2019, § 112). In the 2019 case of Catt v. the United Kingdom, concerning the storage in a police database of data relating to a peaceful demonstrator, the national courts had merely made reference to the general data protection law in examining the lawfulness of the interference. The Court found a violation of Article 8, pointing out that the sensitive nature of the data in question should have constituted a key element of the case before the domestic courts, as it was before the Court (ibid., § 112). The Court likewise found a violation of Article 8 in M.D. and Others v. Spain, 2022, (§§ 63-64) concerning a report drawn up by the police in respect of judges and magistrates, who exercised their functions in Catalonia and who had signed a manifesto in which they had set out their legal opinion in favor of the possibility of the Catalan people's exercising the so-called "right to decide", the report revealing, in particular, the political views of some of the applicants.

The right to the protection of personal data revealing the religious or other beliefs, including philosophical, of an individual was examined by the Court in the cases of Sinan Isik v. Turkey, 2010 (§ 37) and Mockute v. Lithuania, 2018 (§ 117). As to the indication of religion on the applicants' identity cards, the Court emphasized the importance of the right to protection of data relating to religious beliefs, which constituted one of the most vital elements making up the identity of believers and their conception of life, as protected by Article 9 of the Convention (Sinan Isik v. Turkey, 2010, § 37).

7.3.5.4. Data revealing trade union membership

Personal data revealing the trade union membership of an individual may also be "sensitive" and thus warrant heightened protection. In the case of Catt v. the United Kingdom, 2019 (§ 112), information had been collected by the police about the applicant's participation in demonstrations organized by a number of trade unions, in particular his name, presence, date of birth and address. In certain cases his appearance had also been described, together with photos taken during the demonstrations in question (ibid., § 10). Engaging in peaceful protest has specific protection under Article 11 of the Convention, which also contains special protection for trade unions (ibid., § 123). While the collection by the police of personal data about the applicant could be regarded as justified, there was no pressing need, in the Court's view to retain the applicant's data, in the absence of any rules setting a definitive maximum time limit on the retention of such data (ibid., §§ 117-119).

7.3.5.5. Genetic and biometric data

The Court has dealt with a number of cases concerning the collection or retention of:

- cellular samples (Van der Velden v. the Netherlands (dec.), 2005; Schmidt v. Germany (dec.), 2006; S. and Marper v. the United Kingdom [GC], 2008; Canonne v. France (dec.), 2015; Caruana v. Malta (dec.), 2018; Trajkovski and Chipovski v. North Macedonia, 2020; Boljevic v. Serbia, 2020);
- DNA profiles (Van der Velden v. the Netherlands (dec.), 2005; Schmidt v. Germany (dec.), 2006; S. and Marper v. the United Kingdom [GC], 2008; W. v. the Netherlands (dec.), 2009; Peruzzo and Martens v. Germany (dec.), 2013; Canonne v. France (dec.), 2015; Aycaguer v. France, 2017; Mifsud v. Malta, 2019; Gaughran v. the United Kingdom, 2020; Trajkovski and Chipovski v. North Macedonia, 2020; Dragan Petrovic v. Serbia, 2020);
- fingerprints (McVeigh, O'Neill and Evans v. the United Kingdom, 1981; Kinnunen v. Finland, 1993; S. and Marper v. the United Kingdom [GC], 2008; Dimitrov-Kazakov v. Bulgaria, 2011; M.K. v. France, 2013; Suprunenko v. Russia (dec), 2018; Gaughran v. the United Kingdom, 2020; P.N. v. Germany, 2020); Willems v. the Netherlands (dec.), 2021);
- palm prints (P.N. v. Germany, 2020);
- Guide on the case law of the Convention – Data protection
- European court of human rights 13/98 Latest update: 31.08.2022
- voice samples (P.G. and J.H. v. the United Kingdom, 2001; Allan v. the United Kingdom, 2002; Doerga v. the Netherlands, 2004; Vetter v. France, 2005; Wisse v. France, 2005).

Data concerning health, sex life or sexual orientation

Information concerning an individual's health constitutes a key element of private life (Yvonne Chave nee Jullien v. France, 1991, § 75; L.L. v. France, 2006; Radu v. Moldova, 2014; L.H. v. Latvia, 2014, § 56; Konovalova v. Russia, 2014, §§ 27, 41; Y.Y. v. Russia, 2016, § 38; Surikov v. Ukraine, 2017; Francu v. Romania, 2020, § 52). Respect for the confidentiality of this information is crucial, not only to respect the sense of privacy of a patient but also to preserve his or her confidence in the medical profession and in the health services in general. These considerations are especially valid as regards protection of the confidentiality of information about a person's HIV infection. (Z v. Finland, 1997, § 96; Kiyutin v. Russia, 2011, § 64; Armoniene v. Lithuania, 2008, § 40; Biriuk v. Lithuania, 2008, § 39; I. v. Finland, 2008, § 38; C.C. v. Spain, 2009, § 33; Y. v. Turkey (dec.), 2015, § 65; P.T. v. Republic of Moldova, 2020, §§ 5-6, 26; Y.G. v. Russia, 2022, § 45). The disclosure of such data may dramatically affect his or her private and family life, as well as social and employment situation, by exposing him or her to opprobrium and the risk of ostracism (Z v. Finland, 1997, § 96; C.C. v. Spain, 2009, § 33; P. and S. v. Poland, 2012, § 128; Avilkina and Others v. Russia, 2013, § 45; Y. v. Turkey (dec.), 2015, § 65; Y.G. v. Russia, 2022, § 45).

7.3.6. Proportionality tests

Whether the interference was lawful

The Court has examined in a number of cases the question whether the requirement, as stated in Article 5 of Convention 108, that personal data undergoing automatic processing must have been obtained and processed fairly and lawfully, has or has not been met. In a number of cases the Court has found a violation of Article 8 solely on the grounds of a lack of legal basis at national level to authorize measures capable of interfering with the relevant rights (Taylor-Sabori v. the United Kingdom, 2002, §§ 17-19; Radu v. Moldova, 2014, § 31; Mockute v. Lithuania, 2018, §§ 103-104; M.D. and Others v. Spain, 2022, §§ 61-64).

In particular, in Mockute v. Lithuania, 2018 (§§ 103-104), the Court noted that neither the Government nor the national courts had indicated any provision that could have formed the legal basis for the communication, by the psychiatric hospital, of information on the health of the applicant, who was an adult, to his mother and to journalists. In Taylor-Sabori v. the United Kingdom, 2002 (§§ 17-19), where the applicant had been subjected to police surveillance by the "cloning" of his pager, there existed no statutory system to regulate the interception of pager messages transmitted via a private telecommunications system. In M. D. and Others v. Spain, 2022 (§§ 61-64), the police drew up a report in respect of judges and magistrates, who exercised their functions in Catalonia and who had signed a manifesto in which they had set out their legal opinion in favor of the possibility of the Catalan people exercising a so-called "right to decide", the report revealing the personal data, photographs, professional information and political views of some of them. The Court observed that the drawing up of the report by the police had not been provided for by law, and since the public authorities had used the personal

data for a purpose other than that which justified collection, the mere existence of the police report, which had been drafted in respect of individuals whose behavior had not implied any criminal activity, amounted to a violation of Article 8 of the Convention.

7.3.7. Whether the interference pursued a legitimate aim

In a number of cases the Court has examined whether the requirement, as stated in Article 5 of Convention 108, that personal data undergoing automatic processing must have been collected for explicit, specified and legitimate purposes, has or has not been met. In these cases, the examination of the legitimate aims which may justify interference with the exercise of the Article 8 rights, as listed in paragraph 2, is rather succinct. These aims are the protection of national security, public safety and the economic well-being of the country, the prevention of disorder or crime, the protection of health or morals, or the protection of the rights and freedoms of others. The Court generally confirms the existence of one or more of these legitimate aims invoked by the Government.

The Court has taken the view, for example, that the storage in a secret police register of data on the private life of individuals, then the use of that data in the vetting of candidates for posts of importance for national security, pursued a legitimate aim for the purposes of Article 8, namely the protection of national security (Leander v. Sweden, 1987, § 49). Surveillance of an applicant by GPS, ordered by a prosecutor for an investigation into several acts of attempted murder for which a terrorist movement had claimed responsibility and to prevent further bomb attacks, had in the Court's view served the interests of national security and public safety, the prevention of crime and the protection of the rights of the victims (Uzun v. Germany, 2010, § 77).

7.3.8. Whether the interference was "necessary in a democratic society"

In order to be necessary in a democratic society, any measure interfering with the protection of personal data under Article 8 must meet a "pressing social need" and must not be disproportionate to the legitimate aims pursued (Z v. Finland, 1997, § 94; Khelili v. Switzerland, 2011, § 62; Vicent Del Campo v. Spain, 2018, § 46). The reasons invoked by the Government must be pertinent and sufficient (Z v. Finland, 1997, § 94). While it is for the national authorities to make the initial assessment in all these respects, the final evaluation of whether the interference is necessary remains subject to review by the Court for conformity with the requirements of the Convention (S. and Marper v. the United Kingdom [GC], 2008, § 101).

7.3.9. European Court of Justice (ECJ)

7.3.9.1.Data subject's access right

On 12 January 2023, the European Court of Justice (ECJ) delivered a new ruling in the case C-154/21 Österreichische Post regarding information about recipients of personal data. A citizen requested from the Post of Austria, the main operator of postal and logistics services in Austria, to disclose the identity of recipients to whom he has revealed his personal data. He referred to the GDPR of EU. GDPR provides that the data subject has the right to obtain from the controller information about the recipients or categories of recipients to whom his or her personal data have been disclosed or will be disclosed. In response to the citizen's request, the Austrian Post merely stated that it uses personal data and that it offers those personal data to the trading partners for marketing purposes. The question which has risen is whether GDPR leaves the data controller the choice to disclose either the specific identity of the recipients or only the categories of recipient, or whether it gives the data subject the right to know the specific identity of the data recipients.

The ECJ ruled out that this provision does not provide data controllers with the option to choose between identifying particular recipients or categories of recipients. Instead, when they respond to requests by data subjects, data controllers established in the EU must disclose the real identity of the recipients, unless it is impossible or when they can show that the request for access is evidently ungrounded or excessive.

7.3.9.2. Right to damage compensation and parameters

On the fourth of March 2023, the European Court of Justice adopted judgement in the case C-300/21, UI against Österreichische Post AG, whereas it concluded that the breach of GDPR does not confer right to compensation for individuals. According to the opinion of the Court, Article 82 prescribes defining: (i) "damage", whether material or non-material; (ii) actual infringement of GDPR; and (iii) Causal relation between the two. However, the Court also ruled that the right to compensation according to GDPR cannot depend on individuals that fulfil a particular threshold of "seriousness" which is the case according to the applicable Austrian law.

Among others, ECJ requested clarification whether infringement of GDPR is sufficient to establish right to compensation according to Article 82, and furthermore, whether any compensation for non-material damage may depend on the alleged damage which has "weight" over "disturbance", effectively satisfying certain threshold of "seriousness" according to the Austrian law.

VII.

This judgement is used to set the standard, i.e. guidelines for damage compensation. According to the ECJ reasoning in this case:

- For the right to damage compensation prescribed by GDPR three cumulative conditions must be met, as follows: An infringement of the GDPR, material or non-material damage arising from such infringement and the causal link between the infringement and the damage.
- The infringement of the GDPR is not a request for damage compensation.
- However, the compensation for non-material damage does not depend on reaching a particular threshold of materiality.
- The concerned person should prove that they suffered non-material damages.
- The legal systems of each member state prescribes the rules on assessment of the extent of damages, taking into consideration the principles of equivalence and effectiveness.
- The damage suffered as a result of infringement of the GDPR must be "completely" compensated.
- Such complete compensation does not require punitive damages. [37]

37 https://curia.europa.eu/juris/document/document.jsf?text=&docid=273284&pageIndex=0&doclang=en&-mode=lst&dir=&occ=first&part=1&cid=3810075

08

MODERN-DAY CHALLENGES OF DATA PROTECTION

VIII.

MODERN-DAY CHALLENGES OF DATA PROTECTION

8.1. Technological advances, algorithms and artificial intelligence

In cases concerning the taking and storage by the authorities, for crime-prevention purposes, of fingerprints, biological samples and DNA profiles of persons suspected or convicted of offences, the Court has stated clearly that the use of modern scientific techniques cannot be authorized at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private-life interests (S. and Marper v. the United Kingdom [GC], 2008, § 112). Any State claiming a pioneer role in the development of new technologies bears special responsibility for striking the right balance in this regard (ibid., § 112). Bearing in mind the rapid pace of developments in the field of genetics and information technology, the possibility that in the future the private-life interests bound up with genetic information may be adversely affected in novel ways or in a manner which cannot be anticipated with precision today cannot be discounted (ibid., § 71).

In the Court's view, the rapid development of increasingly sophisticated techniques allowing, among other things, facial recognition and facial mapping techniques to be applied to individuals' photographs, makes the taking of their photographs and the storage and possible dissemination of the resulting data problematic. The domestic courts must take account of these factors in assessing the necessity of the interference with the private life of the person concerned (Gaughran v. the United Kingdom, 2020, § 70). In that case (ibid., §§ 96-98), the Court stressed that modern technology was more complex and that the domestic courts had not given sufficient consideration to this aspect in examining the necessity of the interference with the right to respect for private life of the applicant, whose photograph had been taken by the authorities following a minor offence and had been retained even after his conviction had been erased from the records on expiry of the statutory period.

In Breyer v. Germany, 2020 (§ 88), the Court recognized, in the context of the fight against organized crime and terrorism, that modern means of telecommunications and changes in communication behavior required that investigative tools be adapted. In the Court's view, the obligation for mobile-telephone operators to store subscriber information and make it available to the authorities on request is, in general, a suitable response to changes in communication behavior and in the means of telecommunications.

In Szabo and Vissy v. Hungary, 2016 (§ 68), a case concerning mass surveillance of communications, the Court acknowledged that it was a natural consequence of the forms taken by present-day terrorism that governments would resort to cutting-edge technologies, including the massive monitoring of communications, in order to pre-empt imminent attacks. In this case the Court held that the legislation allowing mass surveillance did not provide the necessary safeguards against abuse, because new technologies made it easy for the authorities to intercept large quantities of data relating even to people not in the category originally targeted by the operation. Moreover, measures of this kind could be ordered by the executive without any control and without any assessment as to whether they were strictly necessary, and in the absence of any effective judicial or other remedy (ibid., §§ 73-89).

In the case of Roman Zakharov v. Russia [GC], 2015 (§§ 302-305), the Court held that the risk of abuse inherent in any system of secret surveillance was particularly high in a system where the secret services and the police had direct access, by technical means, to all mobile-telephone communications. The Court found a violation of Article 8, taking the view that the Russian legal provisions allowing generalized interception of communications did not provide adequate and effective guarantees against arbitrariness and the risk of abuse inherent in any system of secret surveillance.

In the case of Akgun v. Turkey, 2021 (§§ 178-181), where at the time of the applicant's initial pre-trial detention the finding that he had used the encrypted ByLock messaging system was the only evidence which was provided to justify the suspicion, for the purposes of Article 5 § 1 (c), that he had committed an offence, the Court emphasized that the use of such evidence as the sole basis underlying a suspicion could pose a number of delicate issues, since, by their nature, the procedure and technologies applied in gathering this evidence were complex and could accordingly reduce the ability of the national courts to establish their authenticity, accuracy and integrity (see paragraph 373 above).

In the cases Centrum for rattvisa v. Sweden [GC], 2021, § 261, and Big Brother Watch and Others v. the United Kingdom [GC], 2021, §§ 322-323, the Court expressly admitted that the use of a bulk interception regime was not per se contrary to Article 8, in view of the proliferation of threats that States currently faced from networks of international actors, using the Internet for communication, and the existence of sophisticated technology which enabled these actors to avoid detection. The Court nevertheless emphasized that in view of the constant development in modern communication technologies, its usual approach to targeted surveillance regimes would have to be adapted to reflect the specific features of a bulk interception regime, on account of the risk of the bulk interception power being abused and of the legitimate need for secrecy in such operations. In particular the process must be subject to "end-to-end safeguards", meaning that, at the domestic level, an assessment should be made at each stage of the process of the necessity and proportionality of the measures being taken; that bulk interception should be subject to independent authorization at the outset, when the object and scope of the operation are being defined; and that the operation should be subject to supervision and independent ex post facto review.

8.1.2. Internet and search engines

Internet sites are an information and communication tool particularly distinct from the printed media, especially as regards the capacity to store and transmit information (M.L. and W.W. v. Germany, 2018, § 91). In the light of its accessibility and its capacity to store and communicate vast amounts of information, the Internet plays an important role in enhancing the public's access to news and facilitating the dissemination of information generally (Times Newspapers Ltd v. the United Kingdom (nos. 1 and 2), 2009, § 27).

The risk of harm posed by content and communications on the Internet to the exercise and enjoyment of human rights and freedoms, particularly the right to respect for private life, is certainly higher than that posed by the press, particularly on account of the important role of search engines (M.L. and W.W. v. Germany, 2018, § 91 and the references cited therein).

Information containing personal data held by media outlets can easily be found by Internet users via search engines (ibid., § 97). Because of this amplifying effect on the dissemination of information and the nature of the activity underlying the publication of information, the obligations of search engines towards the individual who is the subject of the information may differ from those of the entity which originally published the information (ibid., § 97). Hence, in a case in which two individuals had requested that the full details of their identity and their photographs be removed from the online archives of certain newspapers and radio stations after they had finished serving long prison sentences for murder (ibid., §§ 7, 12, 33), the Court found that the balancing of the interests at stake could result in different outcomes depending on whether a request for the deletion of personal data concerned the original publisher of the information, whose activity was generally at the heart of what freedom of expression was intended to protect, or a search engine whose main interest was not in publishing the initial information about the person concerned, but in particular in facilitating identification of any available information on that person and establishing a profile of him or her (ibid., § 97).

In the Court's view, Internet archives contribute to preserving and making available news and information (Times Newspapers Ltd v. the United Kingdom (nos. 1 and 2), 2009, § 45). Such archives constitute an important source for education and historical research, particularly as they are readily accessible to the public and are generally free.

The case of Biancardi v. Italy, 2021, §§ 67-70, afforded the Court its first opportunity to rule on the compatibility with Article 10 of a civil judgment against a journalist for not de-indexing sensitive information published on the Internet concerning criminal proceedings against private individuals and the journalist's decision to keep the information easily accessible in spite of opposition from those concerned. The question of anonymizing identities in the on-line article did not arise in this case. The Court noted that the article had remained easily accessible online for eight months after a formal request to remove it by the persons concerned. The severity of the sanction - liability under civil and not criminal law - and the amount of the compensation awarded did not appear excessive.

8.2. Data transfers and data flows

In Satakunnan Markkinaporssi Oy and Satamedia Oy v. Finland [GC], 2017, in the Court's view, the existence of a public interest in providing access to, and allowing the collection of, large amounts of taxation data for journalistic purposes did not necessarily or automatically mean that there was also a public interest in disseminating en masse such raw data in unaltered form without any analytical input. A distinction had to be made between the processing of data for journalistic purposes and the dissemination of the raw data to which the journalists were given privileged access (ibid., § 175). In that context, the fact of prohibiting the mass publication of personal taxation data in a manner incompatible with Finnish and EU rules on data protection was not, as such, a sanction, despite the fact that, in practice, the limitations imposed on the quantity of the information to be published may have rendered some of the applicant companies' business activities less profitable (ibid., § 197).

The case of Big Brother Watch and Others v. the United Kingdom [GC], 2021 raised, inter alia, the question of the compatibility with Article 8 of the Convention of the sharing of data intercepted by foreign intelligence services, in this case the US National Security Agency ("NSA"). The Court stated that the exchange of data had to be framed by clear detailed rules which gave citizens an adequate indication of the circumstances in which and the conditions on which the authorities were empowered to make such requests and which provided effective guarantees against the use of this power to circumvent domestic law and/or the States' obligations under the Convention. Upon receipt of the intercept material, the receiving State must have in place adequate safeguards for its examination, use and storage; for its onward transmission; and for its erasure and destruction. These safeguards were equally applicable to the receipt, by a Contracting State, of solicited intercept material from a foreign intelligence service. If States did not always know whether material received from foreign intelligence services was the product of interception, then the Court considered that the same standards should apply to all material received from foreign intelligence services that could be the product of intercept. Finally, any regime permitting intelligence services to request either interception or intercept material from non-Contracting States should be subject to independent supervision, and there should also be the possibility for independent ex post facto review (ibid., §§ 498-499).

VIII.

8.3. Training of actors and bodies within the judiciary

Having into consideration that privacy and data protection are complex issues, the judicial bodies should be adequately trained in this matter. Certainly, this training shall include the Law on personal data protection, as well as all other regulations and acts mentioned in this Guide, with emphasis on ECHR and the case law of the ECHR. More advanced knowledge is necessary in computer science, internet, etc. The time we live in demands a specific focus on the new technologies, such as artificial intelligence.

8.4. Public awareness campaigns

We need public awareness campaigns which will inform people on data protection, the dangers of personal data processing in online-environment and their rights, including the possibility for effective legal remedies and what they should include. Also, this will help involved parties to gain information about their rights, obligations, responsibilities and legal means and remedies for protection of their rights to privacy and their personal data.

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