A GUIDE TO DATA PROTECTION AND PRIVACY

Guidebook

Nevena Ružić
Altai Ismailovi

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

A GUIDE TO DATA PROTECTION AND PRIVACY

Nevena Ružić
Altai Ismailovi
Guidebook
2022

Council of Europe

Contents

This material has been produced within the Council of Europe project "Promoting Media Professionalism and Freedom of Information in Azerbaijan (PRO-M-FEX)". The opinions expressed in this work are the responsibility of the author(s) and do not necessarily reflect the official policy of the Council of Europe.

Cover design and layout:
Express Print LLC printing company

© **Council of Europe,** October 2022
Printed by Express Print LLC
printing company

Intro

How to Use this Guidebook

This guidebook aims to familiarise readers with the key features of data protection regimes in the Council of Europe and the European Union, with reference to national data protection regulations. While it is not exclusively reserved for legal professionals, the primary audience of this guidebook is legal practitioners who can better understand and apply complex international standards and national statutory provisions.

The Republic of Azerbaijan adopted the Personal Data Law in 2010, and it has undergone minimal amendments since then. At that time, the Council of Europe's data protection framework consisted of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (known as Convention 108), which the Republic of Azerbaijan ratified. Additionally, there was an Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, which the Republic of Azerbaijan has not ratified. There were also several recommendations and resolutions pertaining to specific aspects of data protection. Concurrently, the European Union applied the Data Protection Directive 95/46/EC and a few other directives addressing specific aspects of data protection, such as telecommunications.

Since then, the rapid development and reliance on information technologies have led to increased global attention to data protection matters, influencing both international documents and national legislation. The importance given to data protection worldwide is reflected in the establishment of the Special Rapporteur on Privacy by the United Nations Human Rights Council in 2015.

At the Council of Europe level, a new amending Protocol called Convention 108+ was adopted in 2018, raising the European standard in data protection and applying to non-CoE member states that have signed and ratified it. Convention 108+ introduced numerous novel provisions related to the definition of personal data processing, categories of personal data, consent, data subjects' rights, transborder data transfer, and the competencies of independent authorities. In other words, the revision was

significant enough to represent a new set of rules. Convention 108+ is not limited in scope, although Member States have some discretion in restricting its application in the field of national security. However, these exceptions or restrictions cannot undermine the standards set by the Convention regarding the legitimacy of data processing, data security, transparency of processing, or the rights of data subjects. Additionally, the Council of Europe's overall work in this field has been intensified, resulting in the adoption of new recommendations.

At the European Union level, personal data protection has become the responsibility of the EU rather than its Member States, and a new regulation called the General Data Protection Regulation (GDPR) was adopted in 2016 and became effective in May 2018. The aim of the GDPR was to provide a comprehensive and directly applicable set of rules for the regular processing of personal data in both the public and private sectors. It empowers individuals (data subjects) in the exercise of control over their personal data and their rights related to data processing. GDPR has also granted specially designated independent authorities significant power to oversee the implementation of its provisions and impose substantial fines in cases of non-compliance. However, GDPR does not apply to data processing carried out for the purpose of crime prevention or public safety, nor does it cover matters of national security. The former is regulated under the Law Enforcement Directive (LED), which was adopted alongside the GDPR.

These developments have led to the enactment of numerous new data protection legislations across Europe and worldwide.

On Data Protection and Privacy

The right to privacy and the right to data protection are often closely associated, and it is common to consider them as synonymous. However, these rights are distinct from each other.

The right to privacy pertains to aspects that are typically considered outside the realm of the public sphere. It is not solely limited to information. For instance, unauthorized entry into someone's home would likely violate the right to privacy (specifically, the privacy of the home). However, it does not necessarily impact the right to data protection. Many situations involving data processing, such as public registers, would affect the right to data protection without necessarily affecting the right to privacy, especially in its narrow sense. In colloquial terms, the right to privacy refers to aspects of an individual's life that should remain private.

Although this guidebook primarily focuses on data protection standards, it also addresses the right to privacy.

List of Abbreviations

Convention 108:	The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) entered into force on October 1, 1985.
Convention 108+:	The Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 223) was opened for signature on October 10, 2018.
GDPR:	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).
Personal Data Law:	The Personal Data Law of the Republic of Azerbaijan (Azerbaijan Newspaper, No.121, 06.06.2010).

Data Protection Terminology

Understanding the terminology used in data protection is crucial for comprehending various concepts within this field. In many cases, the terminology may appear illogical or distant from common linguistic interpretations. For instance, the definition of "***processing of personal data***" encompasses any operation or set of operations performed on personal data, including collection, storage, preservation, alteration, retrieval, disclosure, making available, erasure, or destruction of, as well as the carrying out of logical and/or arithmetical operations on such data. Therefore, even the act of merely storing data without any further action is considered processing of personal data, subject to relevant laws and international standards.

Given that data protection often requires the application of international rules or adherence to different legal regimes, it becomes crucial to establish a shared understanding of key definitions.

a) What is (personal) data?

- Personal data

According to Convention 108+, the term "personal data" generally refers to any information relating to an identified or identifiable individual. In other words, it encompasses any information that pertains to a natural person who can be identified, either directly or indirectly, through an identifier such as a name, identification number, location data, online identifier, or other specific factors related to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person (GDPR, Article 4(1)).

For instance, personal data includes a person's name, personal identification number, date of birth, email address, image, fingerprint, or nickname. However, personal data also encompasses other pieces of information that may not initially appear to fall under the definition of personal data. This includes opinions about an individual. This, too, qualifies as personal data.

The definition of personal data under the Personal Data Law is provided in Article 2.1.1. It states that personal data refers to any information that enables the identification of a person, either directly or indirectly. However, it should be noted that this is not the sole definition of personal data in Azerbaijani legislation. Other laws, such as the Law on Access to Information, may have narrower definitions, as stated in Article 3.0.2. Nonetheless, for the purposes of data protection regulations, the definition outlined in the Personal Data Law should be considered applicable in all cases.

The *Personal Data Law* makes a distinction between confidential and open categories of data. According to Article 5.3, open personal data are those that have been declared open by the data subject or have been entered into the information system with the data subject's consent. The data subject's name, surname, and patronymic are considered permanently open personal data. If data is categorised as open, the law does not require it to be treated as confidential. However, regardless of the data's status, the data protection regime still applies.

- Special category of data

A special category of data refers to data that, due to their value to an individual, require special treatment or, in other words, more careful handling. The definition of these data may vary.

According to Convention 108+, this includes genetic data, personal data relating to offences, criminal proceedings, and convictions, as well as related security measures. It also includes biometric data uniquely identifying a person, as well as personal data that reveal information about racial or ethnic origin, political opinions, trade union membership, religious or other beliefs, health, or sexual life.

GDPR provides a somewhat different list. It includes data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, as well as the processing of genetic data, biometric data for the purpose of uniquely

identifying a natural person, and data concerning health or a natural person's sex life or sexual orientation. Under GDPR, data related to criminal convictions and offences, or related security measures are not considered a special category, although they may only be processed under specific circumstances.

In general, data that fall under the special category require additional requirements for their processing. For example, legislation governing the processing of personal data related to health should provide additional safeguards. Similarly, data relating to one's criminal history or lack thereof may only be processed under certain circumstances.

According to Article 2.1.6 of the Personal Data Law, special category personal data include data related to a natural person's racial or national affiliation, family life, religious belief and faith, health, or conviction. Although Article 9, which sets out the main conditions for the processing of personal data, refers to data characterizing biological characteristics and allowing unambiguous identification, such as biometric data, the processing is subject to general conditions, and the data are not regarded as sensitive.

- Pseudonymised Data

Pseudonymous data are data that cannot be attributed to a specific individual (referred to as the data subject in data protection terminology) without the use of additional information held for the purpose of identifying a person. This additional information is kept separately.

In the case of pseudonymous data, the data subject is unknown to all those who do not have access to the additional information. However, even though the data subject is unidentifiable to the public, pseudonymous data is still considered as personal data and is therefore subject to the data protection regime.

Pseudonymisation is a data security measure used either when required by legislation,

such as in the case of clinical trials, or as an additional measure to prevent risks to data subjects.

The *Personal Data Law* does not contain a specific definition of pseudonymised data or reference to pseudonymisation. However, it is important to emphasize that pseudonymisation is permitted, and in such cases, the Personal Data Law applies.

- Anonymous Data

Unlike pseudonymous data, anonymous data mean that a data subject to whom personal data referred to previously cannot be any longer utilised to identify the person. In other words, re-identification is not possible. Since anonymous data cannot be attributed to a specific data subject, they are not considered as personal data. Therefore, the data protection regime does not apply.

The *Personal Data Law* states in Article 2.1.15 that anonymization of personal data means placing personal data in a situation that does not allow to identify its subject. As noted above, the data protection regime does not apply to anonymous data. However, in some other provisions, it seems that the Law would apply to these data as well. For example, Article 9.13 notes that if the results of the processing of anonymous data relate to data constituting a state secret, the protection of that data shall be carried out in accordance with the legislation of the Azerbaijan Republic on state secrets.

b) What is processing of personal data?

- Processing of personal data

"Data processing" refers to any operation or series of operations carried out on personal data, which includes collecting, storing, preserving, modifying, retrieving, disclosing, making available, erasing, or destroying such data (Convention 108+). As a result, any activity involving personal data, even seemingly passive actions like storing or deleting data, is considered as processing of personal data.

Data Protection Law provides definitions for processing and personal data, as well as specific definitions for certain processing activities such as collection, dissemination, or destruction. These actions should also be considered as processing of personal data.

- Transborder data flow

Transborder data flow or cross-border transmission of personal data, as defined by Article 2.1.16 of Data Protection Law, is indeed an operation that constitutes the processing of personal data. This activity, due to its importance for data subjects, is subject to conditions that aim to ensure appropriate safeguards in order to protect the rights and privacy of data subjects.

c) Who are actors in data protection?

- Data Subject

A data subject refers to a natural person to whom the data pertains. They play a central role in any data protection framework, as data protection primarily concerns individuals.

The right to data protection is an individual right that specifically applies to living persons. While certain national data protection legislation may include provisions regarding the processing of data related to deceased persons, it should not be interpreted as granting rights to deceased individuals. Rather, such provisions serve as practical solutions to address this matter within a single piece of legislation.

In some languages, the term "data subject" is translated as "data owner." However, it is important to avoid using this translation to prevent confusion with ownership and the erroneous assumption that personal data can be bought, sold, or destroyed.

According to Article 2.1.2 of the Personal Data Law, the term "data subject" is defined as

an identified or identifiable natural person whose personal data is collected, processed, and protected.

- Data Controller

According to Convention 108, a controller is defined as a natural or legal person, public authority, service, agency, or any other body that, either alone or jointly with others, holds decision-making power regarding data processing. The crucial aspect is their ability to make decisions.

In certain cases, this decision-making power may not truly rest solely with the controller. For instance, every employer is legally considered a data controller concerning the personal data of their employees. What defines a data controller is that without their presence or intention, there would be no processing of personal data.

Similar to the term "data subject," the term "data controller" is sometimes referred to as "data owner." However, such attribution should be rejected as the data controller is responsible and accountable for every action related to data.

In the *Personal Data Law*, a controller is referred to as the "owner of personal data" in Article 2.1.9. However, it should be understood that this definition does not imply "ownership" over data pertaining to other individuals (data subjects).

- Data Processor

According to Convention 108, a data processor is defined as a natural or legal person, public authority, service, agency, or any other entity that processes personal data on behalf of the controller. Unlike a data controller, a data processor does not have an inherent interest in personal data; their interest lies in their relationship with the data controller.

Typically, data processors are selected by data controllers. However, in some cases, legislation may define the role of data processors. Naturally, data processors do not have the same set of obligations as data controllers.

In the *Personal Data Law*, the term "data protection operator" is defined as a government body, legal entity, or natural person to whom the data owner entrusts specific processing operations. However, it's important to distinguish the role of a "data protection operator" from that of the "owner of personal data," as both roles have distinct responsibilities. Nonetheless, certain duties apply to both equally.

- Data Recipient

According to Convention 108, a data recipient refers to a natural or legal person, public authority, service, agency, or any other entity to whom data is disclosed or made available. Depending on the specific circumstances, the recipient may act as a data controller or a data processor.

In the Personal Data Law, the term "personal data user" is defined as a government body, legal entity, or natural person who has been granted the right to use personal data within the limits specified by the data owner, within the scope of their authority.

- Data Protection Authority

In numerous jurisdictions worldwide, a data protection authority has been established, particularly as an independent body with supervisory powers. In most Council of Europe member states, especially those within the European Union or additional protocols to Convention 108, this authority is provided with sufficient resources to carry out its responsibilities. Some countries with federal systems also have similar bodies at the territorial level, such as Germany or Switzerland. Among other duties, this authority is responsible for overseeing data protection within the country, conducting inspections of specific personal data processing activities,

addressing data subject complaints (including the power to investigate), enforcing data protection rights, and providing guidance to data controllers to ensure compliance with legal requirements and promote awareness.

The Personal Data Law does not establish such an authority but refers to the "relevant executive authority" for the enforcement of data subjects' rights, which can vary. The law assigns certain supervisory functions to the "relevant executive authority." Presidential Decree 275 of 4 June 2010 and Cabinet Decision 161 of 6 September 2010 suggest that, regardless of variation, the "relevant executive authority" will always be a state body. As per paragraph 2 of the Decision of the Cabinet of Ministers on the approval of the "Requirements for the protection of personal data," supervision of these requirements is carried out by several state bodies within their respective powers, including the Ministry of Transport, Communications and High Technologies of the Republic of Azerbaijan, Ministry of Internal Affairs of the Republic of Azerbaijan, Ministry of Justice of the Republic of Azerbaijan, State Security Service of the Republic of Azerbaijan, Foreign Intelligence Service, Special State Protection Service, and Chamber of Control over Financial Markets of the Republic of Azerbaijan.

It is worth emphasizing, even in a guidebook, that the practice of having a single authority has proven to be justifiable for several reasons. A specialized authority, with its expertise and comprehensive perspective, benefits both individuals and data controllers.

d) What are relevant legal documents?

- National legal documents

A challenging aspect of data protection is that it extends beyond a specific branch of law, unlike areas such as insurance law or intellectual property law. Due to the essential role of personal data processing, the range of legislation involved varies across specific fields of work. However, for a data protection specialist, every field is relevant.

In addition to the universally recognized right to privacy as a fundamental human right, many national constitutions also recognize the right to data protection as a human right. Constitutional provisions serve as the basis for national data protection regulations. For instance, Article 32 of the Constitution of the Republic of Azerbaijan establishes the right to personal immunity, encompassing both data protection and confidentiality of communications.

While the Personal Data Law should provide a comprehensive framework for data processing, the legality of specific personal data processing activities is determined by other legislation, such as relevant sector-specific laws. For example, personal data processed by financial institutions should adhere to laws regulating the financial sector, and personal data processed in educational contexts should align with educational laws. The national data protection act clarifies the conditions under which personal data may be processed and outlines the obligations of data controllers.

Appropriate implementation of data protection regulations relies on the application of other laws. Merely having knowledge of data protection law, no matter how thorough, cannot provide answers regarding the necessity of personal data for issuing personal documents, for example. Moreover, data protection remedies often fall under administrative law, making it important to be familiar with laws concerning administrative procedures. The list of these laws can be extensive.

- International documents

The right to privacy is safeguarded by several international treaties that the Republic of Azerbaijan, as a member, is party to, both at the United Nations and the Council of Europe levels.

The International Covenant on Civil and Political Rights, which was adopted in 1966 and ratified by the Republic of Azerbaijan in 1992, protects the right to privacy. According to Article 17 of the ICCPR, individuals should not be subjected to arbitrary or

unlawful interference with their privacy, family, home, or correspondence. They also have the right to legal protection against such interference or attacks on their honor and reputation. This provision is also outlined in the Convention on the Rights of the Child (Article 16), which Azerbaijan ratified in 1992.

Furthermore, Article 8 of the European Convention on Human Rights, ratified by Azerbaijan in 2002, safeguards the right to private and family life, home, and correspondence. The European Court of Human Rights has handled numerous cases related to personal data protection.

The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, established under the Council of Europe in 1981, was the first and remains the sole thematic international treaty specifically addressing data protection. The Republic of Azerbaijan is a member of this treaty, although it has yet to sign and ratify additional protocols concerning independent bodies, as well as the protocol amending the Convention adopted in 2018. The latter aims to adapt the framework to the evolving digital age, with new technologies and increased transborder data flows, while empowering individuals to exert greater control over the processing of their personal data.

Presently, a comprehensive understanding of personal data protection necessitates considering the provisions of the European Union's General Data Protection Regulation (GDPR), often regarded as a gold standard in this domain. Many national laws enacted worldwide have been modelled after or influenced significantly by the GDPR.

Data Protection Principles

Personal data can be processed as long as the processing adheres to data protection principles. While these principles may seem abstract, they entail specific actions that often have tangible outcomes, such as various documentation.

According to Convention 108, personal data undergoing automatic processing must be obtained and processed in a fair and lawful manner. They should be stored for specified and legitimate purposes and not used in ways that are incompatible with those purposes. The data collected should be adequate, relevant, and not excessive in relation to the stated purposes. Accuracy is crucial, and where necessary, the data should be kept up to date. Additionally, the data should be preserved in a format that allows for identification of the data subjects and should not be retained for longer than necessary for the specified purpose. Similar provisions are found in Convention 108+.

The GDPR establishes several principles concerning the processing of personal data, including lawfulness, fairness, and transparency. It emphasizes purpose limitation, data minimization, accuracy, storage limitation, integrity, and confidentiality, as well as the principle of accountability. These principles effectively explain the overall nature of personal data processing.

The Personal Data Law incorporates some of these principles, which are reflected in various articles, such as Articles 4, 8, 9, and 11.

The principle of lawfulness, fairness, and transparency requires that personal data undergoing processing must be processed in accordance with the law. Data controllers, who are responsible for the processing, need to be aware of the risks posed to individuals (data subjects) and be transparent about the processing by informing people that their data is being processed or will be processed.

Lawful processing means that there must be a legal basis for processing personal data, which varies depending on the purpose and circumstances of the processing. The

legal basis for processing can be obtained through the consent of the data subject, a contractual relationship with the data subject, legal obligations, protection of someone's health or other important public interests, or the legitimate interests of the data controller.

In the past, obtaining a data subject's consent was commonly considered a sufficient legal basis for processing personal data. However, it is now recognized that in practice, consent as a legal basis is not only uncommon but also rare. This is due to the requirement of high-quality consent, which must be freely given, specific, informed, and unambiguous. In many everyday activities, obtaining such consent is not feasible, as is the case with employment or interactions with public authorities. Even in a good relationship, a person may not have the freedom to decide not to give their consent.

On the other hand, the legitimate interest of a data controller is an alternative legal basis for many data processing activities. This is because the law cannot anticipate and regulate every relationship an individual may be involved in. For example, securing private business premises and installing video surveillance is based on legitimate interest. The use of many mobile applications for financial transactions also relies to a great extent on legitimate interest. However, both Convention 108+, GDPR, and compliant national laws require a positive balancing test and documentation to rely on legitimate interest as a legal basis for processing personal data.

It is important to note that in certain cases, there may be different legal bases applicable to the relationship between the data controller and the data subject.

Personal Data Law provides for several legal bases as outlined in Article 9.6. These include obtaining written consent, processing based on legislation that specifies the purposes and methods of data processing, processing for scientific and statistical research purposes with mandatory anonymization and processing necessary to protect the life and health of the data subject. Additionally, processing is allowed for what is known as "open category data." However, achieving compliance with this category can sometimes be difficult, if not

impossible, especially considering the prevalence of activities conducted through ICTs and the widespread use of electronic signatures in the country.

Transparency of processing refers to the obligation of a data controller to provide information to data subjects regarding the processing of their personal data. This ensures that data subjects have a certain level of control over their data. While there may be cases where data subjects cannot be excluded from certain types of processing, such as in the case of official registers or bank account information, they are informed about the processing.

Personal Data Law lists information that is presented to data subjects in cases the processing of personal data is based on their consent. According to Article 8.2, these are data that make it possible to identify the subject; data that make it possible to identify the owner or operator who has obtained consent from the subject; the purpose behind the collection and processing of personal data; lists of personal data, consent to process which was given by the subject, and operations to process them; the period of the validity of the subject's consent and terms and conditions for its retraction; and terms and conditions for the destruction or archiving, in a manner identified by legislation, of personal data collected about the subject after the expiration of the storage period of personal data in the relevant information system or after the death of the subject.

The principle of purpose limitation can be considered as the fundamental principle for data processing. Even when fulfilling a legal obligation, there is a purpose behind such provision in the legal system. Ideally, once the purpose is defined, different individuals should arrive at the same answers regarding the legal basis, scope of data, and duration of processing. Depending on available resources, they may choose different security measures.

However, not every purpose can legitimise data processing. The purpose needs to be defined, restricted, and permissible. For instance, a retailer cannot process data for the purpose of public safety, as this falls under the jurisdiction of relevant national

authorities, not private entities.

The principle of data minimisation, also known as proportionality, requires that only the necessary data for achieving the purpose should be processed, and nothing more. For instance, if there is a requirement to maintain a list of apartment owners in a building, it would be excessive to process data about other tenants or their personal relationships.

In fact, there are national regulations that prohibit the processing of unnecessary personal data. For example, Article 12.5 of the Law on Citizens' Appeals prohibits the processing of unrelated personal data. According to the Code of Criminal Procedure, it is against the law, as stated in Article 199, to unnecessarily collect, disseminate, or use information about a person's private life or other personal information that the person considers to be confidential.

The principle of accuracy ensures that no inaccurate personal data are processed. The quality of data and the accuracy of the processing results are dependent on accurate data. While data may not always be up-to-date, it is not necessary to process only current data in every case.

The principle of storage limitation states that data should not be processed indefinitely. In certain situations, the duration of processing is defined by legislation, such as in court proceedings. For example, in many legal systems, a person's criminal record is expunged after a specified period and subject to conditions set by law. Similar provisions exist in education and social welfare laws. The duration of processing may not be explicitly defined by a specific deadline but can be determined by other parameters. In any case, the duration of processing, defined by the purpose, should be known beforehand and periodically assessed.

The principle of data security, encompassing integrity and confidentiality, requires that data be kept safe and that adequate security measures are in place. These measures can be technical, such as physical barriers or encryption, as well as operational, such as training personnel and limiting data access on a need-to-know basis.

The principle of accountability establishes the foundation for responsible data processing by holding data controllers accountable throughout the entire data processing cycle, even if certain processing activities are outsourced to data processors. Demonstrating compliance and accountability often requires documentation, such as conducting a balancing test when relying on legitimate interest as a legal basis, providing notifications to data subjects containing required information, maintaining records of processing activities, and developing rulebooks and training materials for staff members.

Note: The Personal Data Law does not differentiate between the duties of data controllers and data processors, and it may appear that data processors share equal responsibility for ensuring compliance with the law.

Rights of Data Subjects

Whenever personal data is processed, there is a responsibility to uphold the rights of data subjects. These rights have evolved over time and vary across jurisdictions. For example, in many European Union member states, data subjects have the right to data portability, which allows them to receive their personal data in a structured, commonly used, and machine-readable format and transmit it to another controller without hindrance. This right has emerged due to advancements in technology and data processing. Another example is the "right to be forgotten," which is part of the right to erasure and primarily affects online content.

Under Convention 108, data subjects have the right to be informed about the processing of their data, including the identity of the data controller, the purpose of processing, the right to rectification or erasure, and remedies in case their requests are not fulfilled. Convention 108+ includes a similar list of data subject rights, reflecting the impact of information technologies and introducing new-generation rights. For instance, considering the consequences of automated processing, data subjects have the core right not to be subject to solely automated decisions significantly affecting them and have the right to object.

The GDPR also guarantees data subject rights, including the right to be informed, the right of access, the rights to rectification and erasure, the right to restrict processing, the right to data portability, the right to object, rights related to automated decision-making and profiling, as well as the right to seek remedies.

The Personal Data Law specifies the rights of data subjects. According to Article 7, data subjects have the right to be informed about the processing, the identity of data controllers, the scope of data, the purposes, the right to request erasure or destruction of data, the right to prevent further processing, and the right to receive information about the source of collected personal data. They can also request information regarding compliance certificates and exercise other rights. Data subjects have the right to object to data processing, except in cases where processing is mandated by legislation. Finally, they have the right to lodge complaints with the "relevant authority." As already mentioned above, there is no specified data protection

complaints may be referred to various bodies, such as different ministries.

A data controller is given a deadline to comply with data subject's requests, which is, as set under Article 12.4., maximum 7 business days from the date of receipt of the request unless there is need to address a third party. In such a case the deadline may be extended for another 7 business days. In case personal data is shared with a third party, the data controller (or processor) shall inform a third party about the measures taken to comply with the request. Shorted deadline (5 business days) is envisaged for rejecting data subjects' requests pertaining to the processing conducted in accordance with legislation.

The rights of data subjects vis-à-vis the processing of personal data are not absolute, and are balanced against other interests, that can be both private or public. However, to restrict the rights of data subject, such restriction must be provided by law, aimed to protect legitimate interest and necessary in a democratic society. In the words of Article 11 of the Convention 108+, an exception to some (not all provisions of the Convention) is allowed only when it is "provided for by law, respects the essence of the fundamental rights and freedoms and constitutes a necessary and proportionate measure in a democratic society for:

a. the protection of national security, defence, public safety, important economic and financial interests of the State, the impartiality and independence of the judiciary or the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties, and other essential objectives of general public interest;

b. the protection of the data subject or the rights and fundamental freedoms of others, notably freedom of expression."

The European Court of Human Rights has decided on a number of cases pertaining to data protection, which included the scrutiny of the quality of the law, legitimate interests, or necessary limitations of the right to data protection. Conditions for the lawful use of exceptions were first developed in cases related to the state surveillance

of communications, foreseeability of measures that limit one's rights, as well as the need for sufficiently clear nature of the underlying legislation. The Court practice developed through years, understanding that, like in other rights, the state has both negative and positive duties to provide protection of the rights. Some of those key cases are listed at the end of this guidebook.

Duties of Controllers & Processors

As noted above, every processing of personal data results in the accountability of those responsible for personal data, therefore, for data subjects. This responsibility may be described through individual duties of data controllers. These duties may be distinguished between those that are applicable to every data controller and those that apply only to some.

Every data controller must comply with all data protection principles and need to ensure that data subjects' rights are fully applicable. In short, a data controller may process personal data only under a legal basis stipulated in law (consent, legal provision, health, or, in case of other legislation, also contract with data subjects or legitimate interest of a controller) for specified purposes, while scope of data is proportionate for the purpose, and data that is processed is accurate and is stored no longer than required applying appropriate security measures. In addition, every data controller should provide information about data processing to data subjects and should act upon data subjects' requests regarding data referring to them.

Apart from these duties, there are those that may apply under certain circumstances, or depend on, for example, sensitivity of data that is processed, the scale of data, the nature of the data controller or some other significant distinguisher.

Personal Data Law lists several specific duties for data controllers.

According to Article 5.1., personal data are divided in two categories – open and confidential. Such a duty would assume labelling data and, presumably, application of different security measures.

Article 5.5 obliges data controllers, as well as data processors, to ensure that persons, e.g., employees, contractors, that are taking part in any processing activity sign a written commitment vis-à-vis confidentiality of personal data.

Furthermore, Article 8 stipulates the duty to provide information to a data subject if the processing is based on a data subject's consent.

According to Article 9.9., the data controller has the right to entrust the collection and processing of data to the data processor (operator) on the basis of a contract, under the condition of ensuring the protection of personal data, or to act as a processor (operator) himself/herself.

Data controller is also expected to secure a safe cross-border transmission of personal data. This duty, apart from fulfilling the requirements reefing to the national security and the level of protection provided by national legislation of the country to which personal data are transmitted, in particular refers to the security of data, in accordance with Article 14.4.

Finally, according to Article 15, the data controller is responsible for "state registration of the personal data information system". To register, the data controller is required to provide different types of information, such as: the identity of the data controller, legal bases for the creation of the information system, purpose and means of processing, categories of personal data processed, and categories of data subjects. Furthermore, the data controller should provide a general description of security measures, the date when the collection and processing of personal data were started, the scope of personal data recipients, the monitoring and audit mechanisms for the collection and processing of personal data, as well as other related information systems, methods of information exchange with those systems and categories of data exchanged. In addition, the data controller should provide information about the procedures for ensuring the rights of the data subject specified under Article 7.1. In addition, the data controller should provide information regarding categories of personal data transferred cross-border to other states, as well as to international organizations.

Relevant Court Cases

The judgments of the European Court of Human Rights on the protection of personal data, covering various aspects of the subject, serve as an important guide for international and domestic practice. These judgments are essential in terms of clarifying a number of significant issues, such as the collection, use and disclosure of data belonging to different categories, access to personal data, and so on. The Council of Europe maintains updated list - Case Law of the European Court of Human Rights Concerning the Protection of Personal Data – available online.

The following list reflects some of those cases regarding various data protection issues. Please note that many of these cases could be presented under different key words.

- Access to Personal Data

Gaskin v. The United Kingdom, judgment of 7 July 1989, application no. 10454/83. Refusal to grant former child in care unrestricted access to case records kept by social services failed to secure respect for the Convention.

- Balancing Data Protection with Freedom of Expression and the Right to Information

Von Hannover v. Germany, judgment of 24 June 2004, application no. 59320/00. The state has an obligation to protect an individual's image, even for photos taken of public figures in public spaces.

Mosley v. the United Kingdom, judgment of 10 May 2011, application no. 48009/08. The European Convention on Human Rights does not require media to give prior notice of intended publications to those who feature in them.

Khadija Ismayilova v. Azerbaijan, judgment of 10 January 2019, application no. 65286/13. The state failed to comply with their positive obligation under Article 8 to protect the applicant's private life on account of the significant shortcomings in the investigation and the overall length of the proceedings in the case.

- Consent of the Data Subject

Murray v. The United Kingdom, judgment of 28 October 1994, application no. 14310/88. As far as a person suspected of terrorism is concerned, entry into and search of her home for the purpose of effecting the arrest, record of personal details and photograph without her consent does not violate the Convention.

- Correspondence

Malone v. The United Kingdom, judgment of 2 August 1984, application no. 8691/79. Interception of postal and telephone communications and release of information obtained from "metering" of telephones, both effected by or on behalf of the police within the general context of criminal investigation violated the Convention.

Copland v. United Kingdom, judgment of 3 April 2007, application no. 62617/00. The monitoring of an employee's telephone, e-mail and internet usage violated the Convention.

- DNA Database

S. and Marper v. the United Kingdom, judgment of 4 December 2008, applications nos. 30562/04 and 30566/04. A conviction for refusing to be included in the national computerised DNA database, despite the reservations expressed by the state's Constitutional Court regarding the constitutionality of such database as well as no reference to differentiating the period of storage depending on the nature and gravity of the offences committed, is contrary to the right to respect for private life.

- GPS Data

Uzun v. Germany, judgment of 2 September 2010, application no. 35623/05. GPS surveillance of serious crime suspect was justified and not in violation of the Convention.

- Health Data

Surikov v. Ukraine, judgment of 26 January 2017, application no. 42788/06. The collection, retention and use of sensitive health data, including those pertaining to one's mental health, by an employer in considering a promotion and the disclosure of such data to colleagues and during a public hearing violated the Convention.

- Identity

Rana v. Hungary, judgement of 16 July 2020, application no. 40888/17. The case concerned a transgender man from Iran who had obtained asylum in Hungary but could not legally change his gender and name in that country. The Court concluded that a fair balance had not been struck between the public interest and the applicant's right to respect for his private life owing to the refusal to give him access to the legal gender recognition procedure.

- Private Life at Work

Bărbulescu v. *Romania*, judgment of 5 September 2017, application no. 61496/08. Monitoring of an employee's electronic communications amounted to a breach of his right to private life and correspondence.

- Surveillance and Technology

Trabajo Rueda v. *Spain*, judgment of 30 May 2017, application no. 32600/12. Granting police access to computer files containing child pornography material without prior judicial authorisation, in a non-emergency situation, violated the owner's right to respect for his private life.

Benedik v. *Slovenia*, judgment of 24 April 2018, application no. 588/13. Police's accessing of subscriber information associated with a dynamic IP address needed court order, while the national law lacked clarity, offered virtually no protection from

arbitrary interference, had no safeguards against abuse and no independent supervision of the police powers involved.

- Video Surveillance

Antović and Mirković v. Montenegro, judgment of 28 November 2017, application no. 70838/13. Camera surveillance of lecture halls on the premises of an educational institution violated professors' right to privacy.

Useful resources:

There are many resources available online and free of charge that may assist those eager to learn more about the right to privacy and the right to data protection.

Council of Europe Data Protection Website is one such example where a reader can find all relevant data protection instruments adopted under the auspices of the Council of Europe, the rich list of cases briefly explained, news about upcoming events in data protection and so forth. Council of Europe has also developed a free online self-assessed course on data protection (HELP course "Data Protection and Privacy Rights").

As a result of joint work of the Council of Europe (together with the Registry of the European Court of Human Rights), the European Union (Agency for Fundamental Rights and the European Data Protection Supervisor) the *Handbook on European Data Protection Law* was published in 2018 reflecting both the changes brought by Convention 108+ and the General Data Protection Regulation (GDPR). The Handbook is available for download in different languages, free of charge.

For those looking more into the work of the European Union, and particularly in cases of cooperation with partners in the EU Member States that would entail processing of personal data, the useful resources may be found on the website of the European Data Protection Board, as well as the European Data Protection Supervisor. The European Court of Justice, as the EU judicial body, decides in cases pertaining to data protection and has so far developed inspiring practice, not only pertaining one's rights but also the compliance of national provisions with more specific EU regulation, notably GDPR. For those interested, media is regularly reporting on high fines for violation of GDPR set by national data protection authorities.