UDC: 342.738:340.13(497.7)
Professional paper

THE EFFECT OF THE NEW EU REGULATION 2016/679 (GDPR) ON THE NEW LAW ON PERSONAL DATA PROTECTION IN THE REPUBLIC OF NORTH MACEDONIA

Imer ALIU

Ss. Cyril and Methodius University - Iustinianus Primus Faculty of Law - Skopje

Abstract

The new Law on Personal Data Protection in North Macedonia from 2020 transposes the European Union's General Data Protection Regulation (EU) 2016/679 so-called GDPR, applicable as of 25 May 2018.

This paper offers comprehensive coverage of increasingly important area of data protection legislation and is written at a time when the scale and impact of data processing on society is becoming ever more important. This paper is an overview of the key rules, concepts and definitions and an in-depth analysis of the national data protection legislation in North Macedonia.

By analysing the Law on Personal Data Protection in North Macedonia, compeering with the European Union's General Data Protection Regulation and the reality based on the facts that emerge from this research, I hope that this paper creates a useful material for the data protection corpus, a field that deserves to be explored with a considerable attention in the future.

1. Introduction

The right to protection of personal data in the Republic of North Macedonia is guaranteed by Article 18 of the Constitution of the Republic of North Macedonia and the Law on Personal Data Protection. In 2020, the Parliament of the Republic of North Macedonia adopted the new Law on Personal Data Protection, which transposes the General Data Protection Regulation (EU) 2016/679.

Further, in 2021, the Assembly of the Republic of North Macedonia adopted the Law on the Ratification of the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, which created the assumptions for full normative harmonization of the legislation of the Republic of North Macedonia with the legal instruments for the protection of personal data of the Council of Europe.

On August 24, 2021, the full application of the Law on Personal Data Protection began. The Agency and all controllers and processors had an obligation to comply with the personal data protection regulations within the period of 18 months.

When the new Law on Personal Data Protection entered into force, the Law on Personal Data Protection ("Official Gazette of the Republic of Macedonia", no. 7/05, 103/08, 124/10, 135/11, 43 /14, 153/15, 99/16 and 64/18) ceased to be valid. The period of 18 months was a transitional period towards the application of the new Law on Personal Data Protection, during which the controllers and processors of personal data had to undertake appropriate activities of an analytical nature and, through appropriate legal, technical and organizational measures, had to carry out the harmonization of operations with the requirements of the provisions of this Law, while the time limit for compliance expired on August 24, 2021. In order to ensure the full

implementation and operationalization of the new Law on Personal Data Protection, within the same period (as of 24.08.2021), the by-laws provided for by the new Law on Personal Data Protection should have been adopted by the Director of the Personal Data Protection Agency, as well as through a parliamentary procedure to implement the harmonization of all laws and other regulations governing the collection, processing, storage, use and submission of personal data, with the provisions of the new Law on Personal Data Protection. The main goal of the new Law on Personal Data Protection is first to "recognize" the indisputable fact that, unlike in the past, today the processing of personal data is increasingly and more frequently done in an automated (electronic) way.

The new Law on Personal Data Protection is aligned with the current regulation of the European Union on the protection of personal data, and according to the indications of experts in this field, the regulation is quite complex to interpret, not only for data subjects, controllers and processors, but also for those who are better versed in this area. The new Law on Personal Data Protection introduces new decisions in relation to the processing of personal data, the most important of which are: the principle of accountability and responsibility both at the controller/processor level and at the state level; additional obligations of the controllers, i.e. the processors for the establishment of the privacy institute when designing information systems that process personal data and data protection impact assessment of the envisaged processing operations in relation to the protection of personal data; control mechanism of the authorities for the protection of personal data (for example: the Personal Data Protection Agency) for their consultation in relation to proposals for any legal acts or by-laws that include the processing of personal data, as well as emphasizing the independent, autonomous and impartial functioning of the authorities for the protection of personal data.

2. Subject matter of the new Law on Personal Data Protection

The Law on Personal Data Protection, as a legal and institutional framework for the protection of personal data based on the Constitution of the Republic of North Macedonia (Article 18) which guarantees the security and secrecy of personal data, covers the regulation of several areas that depicts a picture of a constructed system that guarantees protection of personal data and privacy. More precisely, the subject matter of the Law on Personal Data Protection, defined in Article 1, incorporates the regulation of: the protection of personal data and the right to privacy in relation to the processing of personal data, and in particular the principles related to the processing of personal data, the rights of the data subject, the position of the controller and the processor, the transfer of personal data to other countries, the establishment, status and competencies of the Personal Data Protection Agency, the special operations for the processing of personal data, the legal remedies and liability in the processing of personal data, the supervision over the protection of personal data, as well as the misdemeanours and misdemeanour proceedings in this area. The protection of personal data by the Law on Personal Data Protection is guaranteed to every natural person free of discrimination based on nationality, race, skin colour, religious belief, ethnic origin, gender, language, political or other beliefs, material status, origin by birth, education, social background, citizenship, place or type of residence or any other personal characteristics (principle of prohibition of discrimination - Article 5).

The Law on Personal Data Protection in Article 6 provides for subsidiary application of the Law on General Administrative Procedure in relation to the procedures and communication regarding the procedures between the Agency and the parties, which takes place in writing, orally or in

electronic form.

3. Definitions of terms of the new Law on Personal Data Protection

The definitions established by Article 4 of the Law on Personal Data Protection determine the essential and legal sense of the terms used in the Law on Personal Data Protection. Some of the terms, that have a dominant use in the Law on Personal Data Protection, are: ”Personal data” means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name and surname, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; Personal data is also home address, credit card number, IP address, consumer habits, fingerprint, ... “Processing of personal data” means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction; ”Filing system” means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis; “Controller” means the natural or legal person, state administration body, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by law, the controller or the specific criteria for its nomination may be provided for by the same law; "Processor of personal data" means a natural or legal person, state administration body, public authority, agency or other body which processes personal data on behalf of the controller; “Consent” of the data subject means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her; “Special categories of personal data” are personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation and "Supervisory authority" is the Personal Data Protection Agency, which has the status of an autonomous and independent public authority.
The new Law on Personal Data Protection also introduces new concepts, such as: “Profiling” means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements; “Pseudonymisation” means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person; “Genetic data” means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an

analysis of a biological sample from the natural person in question; “Biometric data” means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopy data; “Data concerning health” means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status; “Binding corporate rules” means personal data protection policies which are adhered to by a controller or processor established on the territory of the Republic of North Macedonia for transfers or a set of transfers of personal data from the Republic of North Macedonia to a controller or processor in one or more third countries within a group of undertakings(affiliated companies), or group of enterprises engaged in a joint economic activity; "Direct marketing" means any type of communication carried out by any means according to the latest technological developments, with the purpose of imparting advertising, marketing or publicity content targeting directly a specific data subject, as well as processing of personal data which includes profiling to the extent that it is related to this type of communication. The processing of personal data for the purposes of direct marketing is allowed only if the personal data are processed after the data subject has given explicit consent to such processing.

4. Principles relating to the processing of personal data

Through the established principles for the processing of personal data from Article 9, the Law on Personal Data Protection provides precise and clear guidelines for the controllers and processors on the manner of dealing with personal data in the processing procedure, in order to ensure: legality, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, confidentiality and accountability. As a novelty, the Law on Personal Data Protection establishes an obligation for controllers and processors to prove, i.e., to be able to demonstrate, that the processing of personal data is carried out in accordance with the law and the stipulated principles. Therefore, the institution (principle) - accountability, or, in other words compliance, is foreseen. The legal bases for legal processing are determined in Article 10 of the Law on Personal Data Protection, that is, the article defines the legal bases that guarantee the legality of the processing of personal data. The processing of personal data is lawful only if and to the extent that at least one of the following conditions applies: the data subject has given consent to the processing of his or her personal data for one or more specific purposes, processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract, processing is necessary for compliance with a legal obligation to which the controller is subject, processing is necessary in order to protect the vital interests of the data subject or of another natural person, processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

5. Rights of the data subject

Articles 17 to 27 of the Law on Personal Data Protection regulate the rights of the data subjects, which are realized through appropriate communication modalities in the relationship with the controller, and which ensure the subject's protected status: transparent information, manner of exercising rights, information and access to personal data, right to rectification and erasure of personal data ("right to be forgotten"), right to restriction of processing, right to object and automated individual decision-making, including profiling, as well as the restrictions for exercising these rights.

With the new Law on Personal Data Protection, the rights of natural persons are strengthened, and new rights are introduced, such as the Right to erasure (‘right to be forgotten’) and the Right to data portability. The data subject has the right to obtain from the controller the erasure of personal data concerning him or her, whereby the controller has the obligation to delete them within 30 days from the day of submitting the request for erasure, if one of the following conditions is met: the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; the data subject withdraws consent on which the processing is based, where there is no other legal ground for the processing; the data subject objects to the processing; the personal data have been unlawfully processed; the personal data have to be erased for compliance with a legal obligation established by law to which the controller is subject; the personal data have been collected in relation to the offer of information society services.

Right to data portability - The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where: a) the processing is based on consent and b) the processing is carried out by automated means.

Right to rectification – The data subject has the right to obtain from the controller within 15 days from the day of submission of the request, the rectification of inaccurate personal data concerning him or her.

Right to restriction of processing - The data subject has the right to obtain from the controller restriction of processing where one of the following conditions of the Law on Personal Data Protection applies, such as when the accuracy of the personal data is contested by the data subject. When processing has been restricted, such personal data shall, apart from storage, only be processed with the data subject’s consent or for the establishment, exercise, or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest.

Right to object - Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing. In such a case, the controller stops further processing of personal data for such purposes. In the context of the use of information society services and notwithstanding the regulations on electronic communications, the data subject may exercise his or her right to object by automated means using technical specifications.

6. Controller and processor

In order to comply with the new Law on Personal Data Protection, controllers will have to take appropriate actions to improve, upgrade and adjust their established system for the protection of personal data in accordance with this Law. In that context, controllers will have to perform an in-depth analysis of the existing established system for the protection of personal data in the Law on Personal Data Protection that is applicable to the operations for collection, processing, and storage of personal data. When performing the in-depth analysis, the controllers will have to make an assessment that will cover the following issues, such as: catalogue identification of all data filing systems in relation to: purpose of the processing; categories of natural persons (data subjects) and categories of personal data; data transfer to other countries; stipulated storage periods i.e. erasure of the various categories of personal data, detection of the nature, scope, context and purposes of the processing of personal data, as well as the risks of various probability and severity for the rights and freedoms of natural persons (data subjects) resulting from such processing, the position, role, rights, obligations and responsibilities of the data protection officer, the applicable technical and organizational measures and the need for their upgrading and improvement according to the measures provided for in the Law on Personal Data Protection, the documentation for the technical and organizational measures and their alignment according to the provisions of the Law on Personal Data Protection, the contractual norms for the protection of personal data with the processors (determination of the mutual rights and obligations of the controller and the processor), as well as their evaluation in terms of the existing application of the rules for the protection of personal data, the established training system for employees in connection with the protection of personal data, the establishment of the processes for informing about the rights of natural persons (data subjects) and in relation to the manner of their realization, such as the right to: information, access, rectification, erasure, restriction of processing, data portability and objection, the processes of data transfer to other countries and the legal framework on the grounds of which the transfer is carried out, the use of information infrastructure and software applications and the need to upgrade them and adjustment according to the standards and measures provided for in the Law on Personal Data Protection, especially from the aspect of the applicability of technical and integrated data protection (privacy by design and privacy by default), the established system for periodic and internal control of operations for the processing of personal data, profiling processes, as well as the legal and informational framework for those processes, the position, role, obligations and responsibilities of the management and employees in the existing system for the protection of personal data and the need for adjustment according to the rules provided in the Law on Personal Data Protection (principle of accountability). After completing the in-depth analysis, the controllers will have to adopt and apply an Action Plan with planned activities and measures by priority, as well as dynamics for achieving appropriate compliance with the provisions of the Law on Personal Data Protection. After implementing the planned activities and measures from the Action Plan, the controller will have to continuously monitor and check the application of the harmonized system for the protection of personal data, as well as coordinate the activities and actions between the employees and the management in the function of maintaining the system. Within those frameworks, the data protection officer will have a key role in coordinating employees and management, managing communication between employees and management, their training, as well as monitoring and checking the compliance of the system according to the Law on Personal Data Protection.

7. Obligations and responsibilities of the controller and processor

In the Law on Personal Data Protection, the obligations and responsibilities of the controllers and processors of filing systems are regulated by Articles 28 to 47. The controller, in addition to the current obligation to comply with the new Law on Personal Data Protection, has a regular obligation to implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with the Law on Personal Data Protection. Those measures are reviewed and updated where necessary.

8. Data protection by design and by default

With the new Law on Personal Data Protection, in Article 29, two new institutes have been introduced: Data protection by design and by default. Data protection by design and by default stipulates that the controller shall both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as: pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the Law on Personal Data Protection and protect the rights of data subjects; ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. This obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. Such measures shall ensure that by default personal data are not made accessible without the individual's consent to an indefinite number of natural persons. The purpose of introducing the new institutes is not only for greater protection of the data subjects during the processing of personal data by the controllers and processors, but also the introduction of greater protection of the data subjects from their own actions, i.e., when operating independently with their personal data on some platforms or products.

9. Processor of filing system

Where the processor is not the controller, however the processing is to be carried out on behalf of a controller, according to Article 39 of the Law on Personal Data Protection, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the Law on Personal Data Protection and ensure the protection of the rights of the data subject. The controller and the processor enter a contract or other legal act that regulates the processing. Such contract is binding on the processor regarding the controller and sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. The basic elements of the contract are regulated by Article 32 paragraph 3of the Law on Personal Data Protection.

10. Security of processing

According to Article 36 of the Law on Personal Data Protection the controller and the processor are obliged to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: the pseudonymisation and encryption of personal data; the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. One of the technical measures to ensure a level of security and protection of personal data is pseudonymisation and encryption of personal data. Pseudonymisation, according to the definition from Article 4 of the Law on Personal Data Protection, means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

11. Notification of a personal data breach

In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Personal Data Protection Agency in accordance with Article 37 of the Law on Personal Data Protection, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the Agency is not made within 72 hours, it shall be accompanied by reasons for the delay. The processor shall notify the controller without undue delay after becoming aware of a personal data breach. In the same context, when the personal data breach is likely to result in a substantial risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay (Article 38 of the Law on Personal Data Protection).

12. Data protection impact assessment and prior consultation

Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks. The controller shall seek the advice of the data protection officer (DPO), where designated, when carrying out a data protection impact assessment. A data protection impact assessment shall in particular be required in the case of: a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person; processing on a large scale of special categories of data, or of personal data relating to criminal convictions and offences and a systematic monitoring of a publicly accessible area on a large scale. The Agency establishes and makes public (on its website) a list of the kind of processing operations which are subject to the

requirement for a data protection impact assessment. The controller is required to consult the Agency prior to processing where a data protection impact assessment indicates that the processing would result in a substantial risk in the absence of measures taken by the controller to mitigate the risk. Where the Agency is of the opinion that the intended processing would infringe the Law on Personal Data Protection, in particular where the controller has insufficiently identified or mitigated the risk, the Agency shall, within period of up to 60 days of receipt of the request for consultation, provide written advice to the controller and, where applicable to the processor, and may use any of its powers referred to in the Law on Personal Data Protection. That period may be extended by additional 40 days, considering the complexity of the intended processing.

13. Data Protection Officer

Designation of an authorized person for the protection of personal data, status, conditions for designation, position and tasks of the data protection officer are regulated by Articles 41, 42 and 43 of the Law on Personal Data Protection. The new Law on Personal Data Protection assigns more rights and obligations to the data protection officer and thereby further strengthens his or her role in the process of personal data processing. The controller and the processor are obliged to designate an authorized person for the protection of personal data - a data protection officer in any case where: the processing is carried out by a public authority or body, except for courts acting in their judicial capacity, which designate an officer for other processing of personal data that is carried out in accordance with the law; the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale. Apart from the mentioned three categories of controllers and processors of personal data who have a legal obligation to designate an officer, the rest of the entities decide on the designation on a voluntary basis. This is a novelty in relation to the old Law on Personal Data Protection, which excluded from the obligation to designate officers as the only controllers whose data filing system refers to up to ten employees of the controller, or the processing of personal data refers to members of associations established for political, philosophical, religious or trade union purposes. As a novelty, the Law on Personal Data Protection introduces the possibility that a group of undertakings may appoint a single officer, provided that the officer is easily accessible from each establishment within the group, the Agency, and the data subjects (Article 41 paragraph 2). Also, a novelty, foreseen by the Law on Personal Data Protection, is that the officer is determined based on his or her professional qualification, expert knowledge of the legislation and practices in the field of personal data protection (Article 41 paragraph 5). A person may be designated as a data protection officer if he or she: meets the conditions for employment determined by the Law on Personal Data Protection and other law, at the time of designation does have imposed on him/her a conviction by a final court judgement or misdemeanour sanction with a prohibition to act in his/her profession, activity or duty, has completed higher education and has acquired knowledge and skills regarding the practices and regulations for personal data protection, in accordance with the provisions of the Law on Personal Data Protection. The data protection officer may be a staff member of the controller or processor (as well as under the old Law on Personal Data Protection), as the new Law on Personal Data Protection also provides the opportunity for the officer to fulfil the tasks based on a service contract (Article 41 paragraph 6). The controller or the processor shall publish the contact details of the data protection officer and

communicate them to the Agency. In this manner, direct contact is made possible of the data subjects with the officer at the controller/processor for all issues related to the processing of their personal data and for the exercise of their rights according to the Law on Personal Data Protection.

14. Processing of the national identification number

The national identification number of a citizen, in accordance with Article 83 of the Law on Personal Data Protection, shall be processed only: upon prior consent of the data subject, for the exercise of legally binding rights or responsibilities of the data subject and the controller or in other cases stipulated by law. Only after previously obtained approval by the Agency shall a systematic and extensive processing of the national identification number of the citizen be performed. The controller and the processor shall ensure that the citizen's national identification number is duly made visible, printed, or extracted from a filing system.

15. Judicial remedies and liability

Right to lodge a complaint. Protection of the rights of the data subjects determined by the Law on Personal Data Protection, which are violated in the processing procedures, is carried out on two levels: before the Agency based on a submitted request and before the Administrative Court and the Higher Administrative Court, against the Agency's decision.
Every data subject has the right, according to Article 97 of the Law on Personal Data Protection, 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 the Law on Personal Data Protection. For the submitted request, the Agency carries out supervision in accordance with the Law on Personal Data Protection. Every data subject has the right to an effective judicial remedy against a legally binding decision of the Agency, as well as in the case when the Agency has not acted upon the request or has not informed the data subject within three months about the outcome of the procedure upon the submitted request (Article 98 of the Law on Personal Data Protection). Furthermore, every data subject, according to Article 99 of the Law on Personal Data Protection has the right to an effective judicial remedy where he or she considers that his or her rights under the Law on Personal Data Protection have been infringed because of the processing of his or her personal data in non-compliance with this Regulation. The data subject shall exercise its right by filing a lawsuit to the competent court. Any person who has suffered material or non-material damage because of an infringement of the Law on Personal Data Protection, according to Article 101 has the right to receive compensation from the controller or processor for the damage suffered.

16. Misdemeanour provisions

Misdemeanour provisions are systematized in Articles 110 to 116 of the Law on Personal Data Protection. The new Law on Personal Data Protection, contrary to the old one which prescribed fines in fixed amounts for certain misdemeanours, or in a certain range (from-to), divides the misdemeanour into two categories depending on the severity, and has special misdemeanour provisions for video surveillance. Fines in percentage of the total annual income are determined for misdemeanours of both categories.

Misdemeanours of the I category are minor misdemeanour, listed exhaustively in Article 110 of the Law on Personal Data Protection. For these misdemeanours shall be imposed: a) to the controller or the processor – legal entity, a fine amounting up to 2% of the total annual turnover (in the absolute amount) accrued in the business year preceding the year when the misdemeanour was committed or of the total revenue accrued for a period shorter than a year preceding the year when the misdemeanour was committed in case the legal entity started to operate during that year. Misdemeanours of category II are more serious misdemeanours, listed exhaustively in Article 111 of the Law on Personal Data Protection. For these misdemeanours shall be imposed: a) to the controller or the processor – legal entity, a fine amounting up to 4% of the total annual turnover (in the absolute amount) accrued in the business year preceding the year when the misdemeanour was committed or of the total revenue accrued for a period shorter than a year preceding the year when the misdemeanour was committed in case the legal entity started to operate during that year. In accordance with Article 14 of the Law on Personal Data Protection for all misdemeanours defined in Articles 110, 111 and 112 of the Law on Personal Data Protection, the Agency, as the misdemeanour authority, conducts misdemeanour proceedings and imposes misdemeanour sanctions.

Conclusion

The Law on Personal Data Protection ("Official Gazette of the Republic of North Macedonia" No. 42/20 and 294/21), does not fully implement the decisions that will enable the independence of the Personal Data Protection Agency. The Agency does not have all the necessary resources for the effective performance of its functions and powers. In order to emphasize its independent, autonomous and impartial functioning as provided for in Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and the free movement of such data, it is necessary to amend and supplement the Law on Personal Data Protection.
This situation is also noted in the Report on North Macedonia for 2021 of the European Commission, where the following is stated: "The overall functioning of the Agency largely depends on the Ministry of Finance (MF) and the Ministry of Information Society and Administration (MISA). For hiring personnel, the Agency needs approval from the MF, while for promotion of the personnel and for revision of the organizational structure, it needs approval from MISA. This, in a sense, undermines the Agency's ability to function effectively and fully independently." The same is noted in the Report on North Macedonia for 2022 of the European Commission, where the following is stated: "The continued lack of personnel in the Personal Data Protection Agency (PDPA) has a serious negative impact on the implementation of the Law. This also undermines the ability of the PDPA to carry out its tasks effectively and independently."

References

[1]. Constitution of the Republic of North Macedonia
[2]. Law on Personal Data Protection “Official Gazette of the Republic of North Macedonia” no. 42/2020
[3]. Law on Personal Data Protection “Official Gazette of the Republic of Macedonia” no. 7/2005
[4]. Law on general administrative procedure “Official Gazette of the Republic of Macedonia,” no. 124/2015

[5]. 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)
[6]. 2021 Report on North Macedonia, Directorate-General for Neighbourhood and Enlargement Negotiations, European Commission
[7]. 2022 Report on North Macedonia, Directorate-General for Neighbourhood and Enlargement Negotiations, European Commission
[8]. Solove, Daniel J. The Digital Person: Technology and Privacy in the Information Age. United Kingdom: NYU Press, 2004.
[9]. EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide (2nd. ed.). It Governance Ltd. IT Governance Publishing. 2017.
[10]. Lambert, P. (2017). Understanding the New European Data Protection Rules (1st ed.). Auerbach Publications.
[11]. Stephen R Massey, Ultimate GDPR Practitioner Guide (2nd Edition), Demystifying Privacy & Data Protection, Fox Red Risk 2020
[12]. Leo Besemer, Privacy and Data Protection based on the GDPR, Van Haren, 2020
[13].
[14]. Rulebook on the manner for performing supervision („Official Gazette of the Republic of North Macedonia "number. 122/20);
[15]. Rulebook on data transfers („Official Gazette of the Republic of North Macedonia "number. 122/20);
[16]. Rulebook on the process on data protection impact assessment („Official Gazette of the Republic of North Macedonia" number. 122/20);
[17]. Rulebook on the manner of notification of personal data breach („Official Gazette of the Republic of North Macedonia" number. 122/20);
[18]. Rulebook on notification on high-risk personal data processing („Official Gazette of the Republic of North Macedonia" no. 122/20);
[19]. List of types of processing operations that require a data protection impact assessment („Official Gazette of the Republic of North Macedonia" number 122/20);