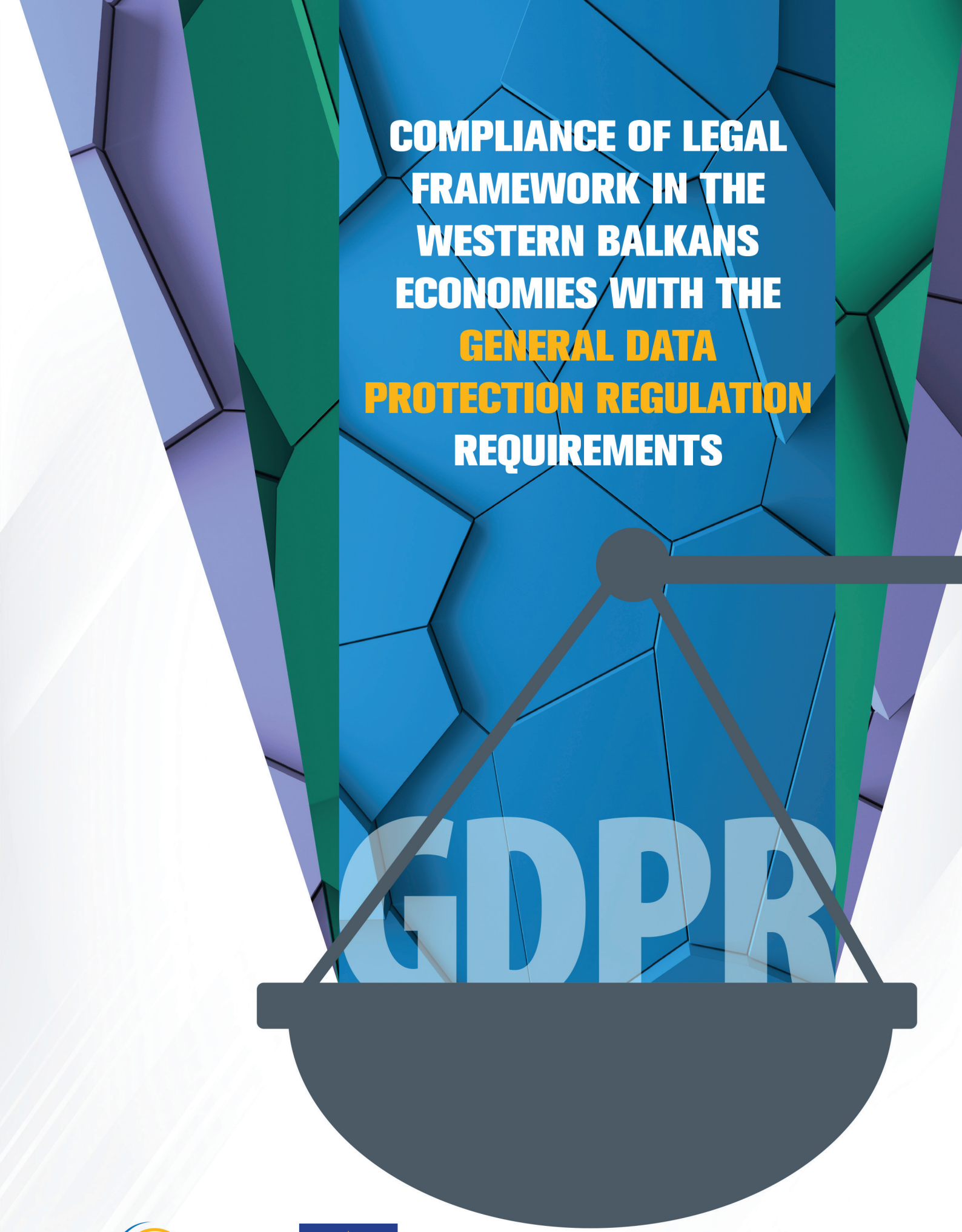
COMPLIANCE OF LEGAL FRAMEWORK IN THE WESTERN BALKANS ECONOMIES WITH THE GENERAL DATA PROTECTION REGULATION REQUIREMENTS



RegionalCooperationCouncil

This project is funded by the European Union

good.
better.
regional.

Title: Compliance of Legal Framework in the Western Balkans Economies With the General Data Protection Regulation (GDPR) Requirements

Publisher: Regional Cooperation Council
Trg Bosne i Hercegovine 1/V, 71000 Sarajevo
Bosnia and Herzegovina

Tel: +387 33 561 700; Fax: +387 33 561 701

E-mail: rcc@rcc.int

Website: www.rcc.int

Authors: Sanja Spasenović, Amina Đugum, Veton Qoku, Goran Radošević, Ljupka Noveska Andonova, all in cooperation with Karanović & Partners, Anisa Rrumbullaku and Urmas Kukk

Editor: Pranvera Kastrati, RCC

Consulting Editor: Milena Jocić-Tanasković and Tanja Maraš, RCC

Design & Layout: Samir Dedić

December 2020

The report is prepared with the financial support of the European Commission.

COMPLIANCE OF LEGAL FRAMEWORK IN THE WESTERN BALKANS ECONOMIES WITH THE GENERAL DATA PROTECTION REGULATION (GDPR) REQUIREMENTS

CONTENTS

*This designation is without prejudice to positions on status, and is in line with UNSCR 1244/1999 and the ICJ Opinion on the Kosovo declaration of independence

INTRODUCTION

The Regional Cooperation Council's project of alignment of the Western Balkans Economies' legislation with the GDPR requirements involves six Western Balkans economies and aims to assess as well as to provide concrete recommendations to ensure proper enforcement at both economy and regional level. The assessment covers all six economies, namely: Albania, Bosnia and Herzegovina, Kosovo*, Montenegro, Republic of North Macedonia and Serbia.

The current level of alignment with the GDPR requirements is not the same in each of the respective economies. Some of them, i.e. Serbia, Kosovo* and Republic of North Macedonia, have already adopted new data protection laws which are modelled after the GDPR and, as such, are generally aligned with the data protection principles and rules envisaged by the GDPR. The remaining economies, Albania, Bosnia and Herzegovina and Montenegro, have not aligned their data protection laws with the GDPR yet, i.e. in each of these economies, GDPR aligned laws are to be adopted. Their adoption in the respective economies is generally expected in the course of 2021.

On the other hand, there are certain characteristics of the data protection environment and practice which are, subject to specifics of each of the respective economies, very similar in all of them. Consequently, challenges in the field of data protection law which are ahead of local data protection authorities, and practical solutions for their overcoming, are generally similar in each of the economies covered by this Data Protection Alignment Project.

Considering the above, the objective of this report is to provide (1) overview of each of the respective economies separately, both from the perspective of their regulatory frameworks (including assessment of their alignment with the GDPR and points of their non-compliance with the same) and practical solutions for overcoming the existing challenges in the field of further data protection development (**Economy Reports**), and (2) overview of the data protection related similarities between the respective economies and, consequently, joint conclusions for further development of their data protection environment (**Key Findings and Conclusions**).

However, before going to the Economy Reports and Key Findings and Conclusions, the report also contains a brief description of the methodology used for its preparing and drafting. Specifically, this is a brief description of the activities undertaken and resources used.

Accordingly, the respective methodology is presented in Part I of this report, Economy Reports for each of the respective Western Balkans economies follow within Part II of the report, whereas assessment for each of them is presented in separate Chapters (one Chapter per economy).

Each Chapter (Chapters I – VI) contained in Part II of the report is consisted of the following five Sections:

1. Current Status;
2. Assessment of the Level of Compliance of the Data Protection Law and Relevant Secondary Legislation with GDPR;
3. Competence of and Challenges in the Work of the Commissioner/Agency;

4. Challenges in the Implementation of the Current Data Protection Law in Private and Public Sector;
5. Crucial Steps for Overcoming the Existing Challenges.

Chapter III, containing Economy Report for Kosovo*, features additional Section, Criteria and Procedure for Selecting the Commissioner[1]. This further means that Chapter III, unlike the remaining Chapters within the Part II of the report, contains six Sections in total.

Part III of the report contains key findings and conclusions providing key findings for the assessment at regional level, including the similarities which exist in the field of data protection environment between the respective Western Balkans economies and consecutively elaborating the joint conclusions.

The last part of the report is Appendix I It contains the list of relevant local structures/ authorities which were contacted to gather information and latest developments in the area of data protection, thus providing their contribution to the report as well as validating the assessments made by the engaged data protection experts. These experts are also listed in Appendix I of the report.

1 This Section is contained only in the Economy Report for Kosovo* as its Section 5.

PART I. METHODOLOGY

The methodology used for preparing and drafting this report is based on the following principal types of activities and resources based on which the respective analyses have been performed:

Activity	Resource
Comprehensive desk analysis of the primary and secondary data protection legislation in each of the involved Western Balkans economies	Access to various legislation databases including the online access to the official gazettes of the involved economies, both at the level of relevant laws and related secondary legislation
Accompanying desk analysis of the comparative and regional overviews in the field of data protection, privacy and information security	Access to various comparative analyses and regional overviews conducted in the past for the purpose of analysing different circumstances in different economies
Combining the findings of the above analysis with the existing accumulated practical know-how for the purpose of identifying challenges in the implementation of GDPR and proposing practical solutions for overcoming the respective challenges in each of the involved economies	Engagement of top-tier data protection experts across the Western Balkans, their cooperation and relevant combination of EU/international expertise and local and regional expertise through engagement of the international expert with over 25 years of experience in the field of privacy and personal data protection law
Structured interviews with institutions/authorities responsible for data protection in each WB economy. The process entailed preparing and providing the questionnaires to be answered by the relevant local structures/authorities in the Western Balkans economies with regard to the issues of crucial importance for further implementation and enforcement of the GDPR requirements	Existing expert knowledge of the engaged data protection lawyers and use of the contacts in relevant local structures/authorities provided by the Regional Cooperation Council
Further communication (verbal/written/on-line meeting) with the relevant local structures/ authorities in each of the Western Balkans economies for the purpose of (1) learning about their position on the current state of play and expected/ required developments in the field of data protection law and (2) identifying the ongoing donor support and projects in the field of data protection/GDPR alignment and capacity building needs in the relevant institutions	Existing cooperation with the respective authorities and use of contacts provided by the Regional Cooperation Council, as well as communication with the engaged international expert
Comprehensive analysis of publicly available data and documents, including but not limited to information/reports/opinions published by the local data protection authorities in the Western Balkans economies	Access to publicly available data and documents in the involved economies along with the use of engaged data protection experts' knowledge and practice in the field of data protection law

PART II. ECONOMY REPORTS

CHAPTER I. ALBANIA

1. CURRENT STATUS

The law no. 9887 dated 10 March 2008, as amended, on the Protection of Personal Data ("**Current Data Protection Law**") represents the main legal act regulating data protection and privacy in Albania. The Law entered into force in 2008 to replace the old law of 1999 and was since then amended twice, in 2012 and 2014 respectively.

The competent authority for data protection matters in Albania is the Commissioner for Protection of Personal Data ("**Commissioner**"). The Commissioner is seated in Tirana and the official website is www.idp.al Further information on the organisation, competence and challenges it faces in its work is provided in Section 3 herein.

The Current Data Protection Law and related secondary legislation, as described in further details in Section 2 of Chapter I herein, mirror some of the provisions of the EU Data Protection Directive (95/46/EC). However, it is not fully aligned with the GDPR.

Nevertheless, the fact that GDPR entered into force and began to apply in May 2018 led to positive developments in Albania.

Specifically, in 2019, the Parliament of Albania, in its Draft Resolution "On Assessing the Activity of the Information and Data Protection Commissioner for 2019", requested support from the Commissioner in drafting the legal acts and bylaws necessary to align the data protection framework with the EU legislation and specifically the GDPR and the Police Directive 2016/680.

In this regard, the Commissioner stated in the 2019 Annual Report of the Commissioner's Office that it has carried out all the preparatory work and procedures to be followed for the implementation of a twinning project funded by IPA 2017 programme of the European Union the purpose of which is the approximation of the domestic legislation with the GDPR and the Police Directive. According to the discussions with the Commissioner, the implementation of the respective project started in October 2020.

When it comes to the new law's drafting process, according to the Commissioner it has already started and is expected to be completed in/around September 2021.

In any case, partial alignment interventions have been made by the Commissioner through secondary legislation such as the adoption of the Commissioner's Guideline no.48 as of 2018 "On the certification of systems managing information security, personal data and their protection".

Overview of the main challenges in the implementation of the data protection law in Albania, both on the side of the Commissioner and on the side of local data controllers/processors ("**Local Processing Entities**") is provided in Section 4 of Chapter I herein. Identification and description of crucial steps for overcoming the respective challenges follows in Section 5.

2. ASSESSMENT OF THE LEVEL OF COMPLIANCE OF THE DATA PROTECTION LAW AND RELEVANT SECONDARY LEGISLATION WITH GDPR

This overview contains a summary of the legal framework on data protection, specifically primary legislation, including the Constitution of Albania and the Current Data Protection Law, as well as the most relevant secondary legislation. The bylaws include several decisions, guidelines, and instructions of the Commissioner.

Main topics to be covered by this overview of the respective legislation include the following: (1) general data processing requirements, (2) obligations and responsibility of data controllers and data processors, (3) data protection officers and representatives of foreign entities, (4) special categories of personal data, (5) rights of data subjects, (6) registration of data processing activities, (7) data breach related notification and data protection impact assessment, (8) data transfer, (9) penal policy, and (10) relevant secondary legislation.

1. GENERAL DATA PROCESSING REQUIREMENTS

According to the Current Data Protection Law, all processing of personal data should be made based on the following principles: (1) processing of data should be fair and based on legal grounds, (2) collected and processed data should be accurate and up to date to avoid inadequate or incomplete data, (3) personal data should be adequate, which means relevant as to the purpose of their processing and not excessive in relation to such purpose, (4) personal data should be collected for a specific, clearly stated and legitimate purpose and shall be processed in a way that is compatible with such purpose, (5) personal data should be kept for only as long as necessary to satisfy the purpose for which the data was first collected and then further processed, (6) for the purpose of data processing, all required safety measures, organisational and technical, as provided under the Current Data Protection Law, should be in place.

The aforementioned measures include: defining organisational unit functions and operators for the use of data; using data only upon orders of organisational units or authorised operators; instructing operators on the obligations they have in relation to the Current Data Protection Law; permitting access to data and programmes only by authorised persons, etc.

The lawfulness principle, provided under (1) above, requires for the processing of personal data to be made based on the legal grounds governed by the Current Data Protection Law. Such legal ground is either the consent of data subject or one of the remaining grounds expressly provided by the Current Data Protection Law.

Specifically, these grounds include:

1. Necessity of processing for the performance of a contract where the data subject is a party to or, in order to negotiate or amend a contract at the request of the data subject;
2. Protection of the data subject's vital interests;
3. Performance of a legal duty of public interest or exercise of powers of the controller or of a third party to whom the data are disclosed;
4. Necessity of processing for the protection of the legitimate rights and interests of the data controller, data recipient or any other interested party provided however that processing in this case cannot override the right of data subject to protection of personal life and privacy.

While the above principles are in line with the processing requirements provided under the GDPR, the comparison of the provisions of Current Data Protection Law and GDPR

shows that GDPR has paid significant attention to the broader listing of these principles in comparison to those of the Albanian legislation. For example, the principles related to the transparency of the processing and integrity and confidentiality are explicitly provided for under Article 5 of the GDPR. However, although such principles are not explicitly mentioned in the Current Data Protection Law, it is understandable that the spirit of this law, and the secondary legislation issued on its bases, requires that the processing should be done in a transparent manner in relation to the data subject, as well as in a manner that ensures the appropriate security of personal data (integrity and confidentiality).

In addition, Article 28 of the Current Data Protection Law provides for the obligation of the data controller and data processor to preserve confidentiality of personal data, while the Instructions no. 22 and 47 provided in Section 2, item 10 below, set out that the processing (and archiving) of personal data by any (small and/or large) data controller should account to the principles of confidentiality and integrity of processing.

In relation to the consent to be obtained from the data subject, the Current Data Protection Law sets out that it should be given in writing. On the other hand, GDPR, as regards the form, does not limit it to the written form. However, if it is given in written, Article 7 of the GDPR provides that, in such, case the data controller should present the request for the consent in a manner that is clearly distinguishable from other matters (i.e. in case is will be obtained in context of, inter alia, a contract or document that concerns also other matters), as well as in an intelligible and easily accessible form (i.e. using clear and plain language). GDPR, as opposed to the Current Data Protection Law, pays close attention to the assurance of understanding that a data subject is going to have when requested (by a data controller) to consent the processing of relevant categories of his/her personal data and/or to consent the categories of processing (i.e. retention, disclosure, etc.). Should the content of the consent fail to 'pass' such test of intelligibility and clearness, it might be considered as infringement of the GDPR provisions and, therefore, null and void.

In addition, another novelty of the GDPR is the introduction of the consent applicable to children in relation to the information society services. To give his/her consent the child should not be younger than 16 years; otherwise the consent is valid if provided by the holder of parental responsibility over the child. GDPR grants discretional room to the member states to provide for a lower age, provided that is not below 13 years.

Albanian legislation on personal data deals specifically with child's consent rules in cases of information society services. Hence, it might be implied that the Albanian legislation requires that the processing of personal data of minors should be carried out only upon consent of the respective holders of parental custody (for any sort of processing).

Having said this, it might be concluded that there are no major differences between GDPR and the Albanian legislation as regards the principles of personal data processing. The elements of the lawfulness of the data processing provided for under the Article 6 of GDPR and Law on Personal Data Protection appear to be at the same level of alignment. However, the Current Data Protection Law does not clearly or comprehensively mention the relevant data protection principles and/or data processing lawfulness requirements as does the GDPR, and some of these principles, as noted above, are vaguely scattered throughout other provisions of the Current Data Protection Law and the secondary legislation enacted by the Commissioner. Therefore, from a point of view of legislative technique, amendment of the relevant provisions of the Current Data Protection Law is recommended in order to implement a clear, transparent and understandable GDPR compliant framework.

2. OBLIGATIONS AND RESPONSIBILITY OF DATA CONTROLLERS AND DATA PROCESSORS

Under the Current Data Protection Law, data controllers and data processors have the obligation to document technical and organisational measures that ensure the protection of personal data in compliance with the legal framework. The security levels should follow the nature of personal data processing activities. It seems that this requirement mirrors the accountability principle provided under the GDPR, however it is not as strong as in the GDPR as it puts no emphasis on the obligation of data controllers and data processors to be able to demonstrate what they did in terms of compliance with the data protection requirements and their effectiveness when requested.

When collecting personal data, data controllers or data processors on behalf of data controllers are obliged to inform the data subject on the scope and purpose of data processing and provide relevant information on the person who is going to process the data and on the means of processing. This obligation does not apply in case the data subject is already aware of such information. The data subject should also be notified on his/her right to access and correct his/her personal data.

If data is obtained by the controller from the data subject himself/herself, the latter should be informed on whether such provision of personal data is mandatory or not. Even when personal data are not obtained from the data subject himself/herself, the controller is not obliged to inform the data subject if data processing takes place for historical, statistical or scientific research purposes; if it is mandatory for the controller to process such data based on a legal provision; if data being processed are public or if the data subject has consented to the processing of his/her data.

Data controllers are also obliged to block, correct or delete personal data being processed if the latter are deemed inaccurate, incomplete, false or have been processed in contradiction with the provisions of the Current Data Protection Law, either by request of the data subject or based on the controller's initiative. The controller is also obliged to inform the recipient of personal data on the correction or deletion of the transmitted data.

Controllers are also entitled to engage processors (outsourcing). Under the Current Data Protection Law, data controllers may hire a data processor to lawfully process personal data as instructed by the formers. In such case, the data controller has the obligation to enter into a written agreement with the data processor. This contractual relationship is further regulated by Instruction no.19 of the Commissioner "On regulation of the relationship between the controller and the processor in case of delegation of personal data processing and master contract form for such legal arrangements". To ensure that the processor fulfils his/her obligations, the controller can request from the processor to provide all relevant information that demonstrate compliance. Data processors should process data based on the instructions of the controller as agreed in the respective contract. In this regard, the processor should not transmit data, unless instructed to do so by the controller, and should notify the controller on the results of the processing. The processor is required to take all the required safety measures and employ operators that are bound by confidentiality obligations. In agreement with the controller, the processor should create technical and organisational conditions for the controller to fulfil his/her obligation to ensure exercise of data subject's rights.

Lastly, under the Current Data Protection Law all data controllers have the obligation to notify the Commissioner of the data processing for which they are responsible, even before such processing takes place for the first time or, in case of change of the processing activities, to notify the Commissioner of such changes. The notification is made through a notification form approved by the Commissioner and submitted online or in soft copy to the Commissioner. It is a standard form which comprises the name and address of the controller, scope of processing, categories of data subjects and categories of personal data, processors and categories of processors of personal data, international transfers the controller intends to operate, and finally a general description of the safety measures for the protection of personal data.

As noted above, both legal acts (i.e. Current Data Protection Law and GDPR) provide for similar definitions of the data controller and data processor. The main responsibilities as regards the lawfulness of personal data processing remain with the personal data controller. The relationship between the data controller and data processor is governed by a contract that sets out the rights and obligations of the parties. However, there are important differences between both legal acts.

According to the Albanian legislation, all data controllers are obliged to notify the Commissioner prior to commencement of the processing of the intended personal data or in case of changes related to such processing (i.e. new categories of data/data subjects, new scope, etc.), while GDPR does not foresee this.

In both jurisdictions, the processing of personal data by the data processor is to be done only in accordance with the instructions of the data controller. As regards this obligation, GDPR provides for an exemption from such obligation in cases when EU or the respective member state, to which the data processor is subject, requires the relevant processing (i.e. irrespective of the instructions of the data controller). Nonetheless, according to GDPR, the data processor is obliged to notify the data controller about such legal requirement before starting the processing of personal data. The Albanian legislation does not provide for such an explicit obligation of data processor to notify the data controller before processing personal data about the relevant legal requirements that would oblige the data processor to disregard the instruction of the data controller.

In addition, according to GDPR, the data processor also has the obligation to assist the data controller in order for the latter to comply with the provisions of GDPR (i.e. including, but not limited to, as regards the security measures, audit, inspections that might be conducted by the data controller, etc.). The obligation for assistance is not specifically provided for under the Albanian legislation. However, it might be stipulated under the processing contract between the parties.

Moreover, according to GDPR any data controller having 250 or more employees is obliged to keep written records of their processing activities (i.e. including, but not limited to, the purpose of processing, description of categories of data subjects and those of personal data, etc.). Such obligation applies also to the data processors for all processing activities performed on behalf of the data controller.

On the other hand, Albanian legislation sets out that the data controller/processor is obliged to register and document the personal data modifications, rectifications, deletions, transmitting, etc. (Article 27 of the Current Data Protection Law). Hence, as it might be noted, there are no applicable thresholds under the Albanian legislation as regards the keeping of records of processing activities.

Concerning the right of the data subject to compensation for damages, according to GDPR data processor is obliged to pay damage relief (to the data subject), if it has not complied with the provisions of GDPR dealing with the activities/obligations of the data processor and/or if it has acted in breach of the instructions of the data controller. Pursuant to the Albanian legislation, the data subjects are entitled to seek compensation from the data controller for the damages incurred due to the unlawful processing of their personal data. However, the processor remains responsible in case of damages incurred by the data subject due to the breach of confidentiality.

3. DATA PROTECTION OFFICERS AND REPRESENTATIVES OF FOREIGN ENTITIES

The appointment of a data protection officer ("**DPO**") is not mandatory although all controllers in Albania are required to have a person appointed as contact person with the Commissioner for their data protection/processing activities.

However, as per Instruction no. 47, as of 14 September 2018 "On the determination of rules on the safety of personal data processed by large controllers", large data processing entities in Albania are required to appoint the DPO that should meet the criteria set out in this Instruction. According to the Instruction, large data processing entities are considered controllers or processors that process data by automatic or manual means, by employing six or more persons, directly or by virtue of the processors. These large controllers/processors must authorise in writing at least one contact person responsible for carrying out the internal supervision of protection of personal data processed and notify such contact person to the Commissioner along with the notification of their data and their processing activity. The main legal criteria to be met by a contact person are for him/her to: (1) have full legal capacity to act, (2) enjoy integrity, (3) have a university degree in law or computer sciences, (4) be known for professional skills, ethical and moral pure figure, (5) have a working experience of not less than 5 years as a lawyer or IT expert, or has worked for more than 3 years in the Commissioner's office in the position of a lawyer or IT expert, and (6) has not been previously convicted of a criminal offence.

The DPO's main responsibilities are: (1) to internally monitor the fulfilment of the obligations for the protection of personal data by the processing entity, (2) to advise the responsible persons on personal data protection, (3) to implement technical and organisational measures in relation to the staff and oversee their implementation in practice, (4) to internally monitor, in case a data controller has contracted a data processor, the activity of the processor and the contractual obligations of the parties, (5) to handover the documentation on the archiving systems for special registration, for announcing changes and de-registration of archiving systems from the special register. The DPO also keeps data on the archiving systems that are not subject to registration and makes them available to any person who has the legal right to access them, (6) cooperate with the Commissioner, (7) to submit, upon request of the Commissioner, the written authorisation based on which he/she operates and proof of the skills acquired during professional training, (8) to monitor the international transfer of personal data.

Public authorities also need to appoint the DPO and notify the Commissioner in writing of this appointment.

The DPO might be removed from office, inter alia, by the data controller and/or upon request of the Commissioner in case of nonfulfillment of the appointment criteria, failure to sufficiently accomplish his/her tasks, and/or in case of erroneous assessment or erroneous implementation of rights and obligations of the data controller.

Considering the above rules on the DPO, it can be concluded that the concept of its appointment is not entirely the same as under the GDPR (although the purpose of its appointment is substantially the same as under the GDPR). Specifically, the GDPR governs that the DPO's appointment is obligatory in three cases (based on the fact that particular types of data are processed or that, regardless of the processed data type/-s, the processing is carried out by public authorities), while it is voluntary in all other. For the sake of completeness, the cases when the respective appointment is necessary under the GDPR are the following:

1. Processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
2. Core activities of the data controller/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, and
3. Core activities of the data controller/processor consist of processing on a large scale of so-called special categories of data and personal data relating to criminal convictions and offences.

In respect of representatives of foreign entities, as noted in Section 2, Item 1 of this Report, the Current Data Protection Law applies, inter alia, to data controllers which are seated outside the territory of Albania, but exercise their activity using means (equipment) located on the territory of Albania. In such case, the controllers must designate a representative on the territory of Albania. In other words, the concept of/reasoning behind the respective designation differs completely from the respective concept/reasoning envisaged by the GDPR (for example, one of the cases when such appointment is obligatory under the GDPR is the case when a non-EU entity offers services to natural persons in the EU, whereas it is irrelevant whether any equipment which such entity uses for the respective data processing is located in the EU).

4. SPECIAL CATEGORIES OF PERSONAL DATA

The Current Data Protection Law regulates 'sensitive' rather than 'special categories of personal data' as under the GDPR.

Accordingly, sensitive data according to this Law includes any piece of information related to a natural person that reveals his/her racial or ethnic origin, political opinions, trade union membership, religious or philosophical beliefs, criminal prosecution, as well as data concerning his/her health and sexual life. Sensitive data in the Current Data Protection Law do not expressly include genetic or biometric data.

Any processing of sensitive data is expressly prohibited. Processing of sensitive data is allowed in certain exceptional cases prescribed by the Current Data Protection Law. For example, processing is permitted if the data subject has given his/her consent which can be revoked at any time making further processing of such data illegal; the processing of personal data is in the vital interest of the data subject; processing is authorised by the responsible authority for an important public interest, under adequate safeguards; processing is related to data that are manifestly made public by the data subject; processing is related to data that are processed for historic, scientific or statistical research; the data are required for the purposes of preventive medicine, medical diagnosis, etc.; data are processed by non-profit organisations and trade unions for purposes of their legitimate activity; and, lastly when data processing is necessary for the purpose of accomplishing a legal obligation and a specific right of the controller in the field of employment.

If any of the conditions above is fulfilled sensitive data can be processed without having to obtain an authorisation from the Commissioner. Otherwise, if none of the conditions above are met, sensitive data can only be processed if the data controller obtains an authorisation to do so from the Commissioner. In any case, it is mandatory that a data controller/processor notifies its intent to process sensitive data in the notification form filed with the Commissioner.

5. RIGHTS OF DATA SUBJECTS

The Current Data Protection Law foresees some main rights of data subjects, as follows: (1) right to access the information being processed: every data subject is entitled to obtain from the data controller, upon his/her written request and free of charge, information on whether his/her data is being processed or not, the purpose of processing, the categories of processed data and to whom that information is disclosed. He/she is also entitled to know what data is being processed and their source, if applicable. In case of automated decisions, the data subject is entitled to be informed on the logic applied in the decision-making. The data controller shall, within 30 days from the date of the receipt of the request for information, inform the data subject or explain the reasons for withholding such information; (2) right to request blocking, rectification and deletion: anyone whose data is being processed has the right to request blocking, rectification or deletion of his/her data, if the data relating to him/her are either irregular, false and incomplete or have been processed contrary to the law; (3) right to object processing: the data subject has the right to refuse the processing of his/her data at any time, free of charge. This means he/she is entitled to demand the data controller to not start processing or, if the data processing has already started, he/she can request from the controller to stop the data processing; (4) right to complain: every person claiming that his/her rights and/or legal interests with relation to his/her personal data have been infringed can file a complaint or notify the Commissioner and request its intervention. Following that, the data subject can also claim in court for the infringed right; (5) right to compensation: everyone whose data has been processed unlawfully is entitled to compensation for damages based on the Civil Code of Albania; (6) every data subject has the right not to be subject to decisions based only on automatic processing of data (automated decision) that cause legal effects or that affects him/her by assessing certain personal aspects related to him/her, particularly his/her work efficiency, credibility or behaviour.

The Current Data Protection Law does not foresee provisions related to the two novelty rights introduced by the GDPR such as the right to be forgotten (although it does recognise the right to deletion as such, as mentioned above) and the right to data portability.

In addition, concerning all other data subject rights, there are some other notable differences between the GDPR and Current Data Protection Law as noted below.

Right of information

Both Current Data Protection Law and the GDPR provide for the obligation of the data controller to inform the data subject on the processing of his/her personal data, when carrying out such processing. However, the provisions of GDPR (i.e. Articles 13 and 14) contain detailed and specific requirements as regards the proper information of the data subject. E.g. GDPR explicitly differentiates between the information obligations in relation to data directly collected (processed) by the data subject (i.e. direct collection) and the obligations in relation to data collected from other sources (i.e. not directly from the data subject – indirect collection). Further, the information that should be given to data subjects according to the GDPR is far more complete than that prescribed by the Albanian law. It provides for, inter alia, the obligation of data controller to provide the contact details of the DPO, the legitimate interest of data processing (if applicable) pursued by the data controller (or by a third party), a thorough information on international transfer of personal data (including the information on appropriate safeguards, etc.), the criteria used to determine the retention period, the right to withdraw the consent given at any time (if applicable), information on automated decision-making – including profiling – (if applicable), the source of the personal data (when they are not obtained directly from the data subject). In addition, GDPR sets out specific requirements regarding timing of information to be provided to the data subject when the personal data are not collected from the latter.

On the other hand, except for personal data processing for direct marketing purposes, the Current Data Protection Law does not provide for a different treatment of the collection of personal data directly from the data subject and indirectly. It only states that when collecting personal data, the data controller should inform the data subject on the elements listed under Article 18 of the Current Data Protection Law. Lack of specific timing regarding the information to be provided to the data subject regarding the indirect collection of personal data has led in practice to data controllers believing that they are not obliged to provide any information at all to the data subjects in case the personal data are not collected directly from them.

As regards direct marketing, the controller that collects the data not directly from the data subject is obliged to undertake some steps to ensure that the latter are aware of the information that would have been provided to them if their personal data would have been collected directly from them. Such information should be given as of the time of processing of personal data for marketing purposes. However, also in case of direct marketing, the

Albanian legislation does not indicate the steps to be taken by the data controller in order to provide information to the data subjects on the data not collected from the latter.

Other rights

When comparing the rights of data subjects provided for under the Albanian legislation with those of GDPR, other differences are noted in respect of (i) the right to restrict processing; (ii) the right to data portability (iii) the right to object the automated decision-making; (iv) the right to object direct marketing; and (v) the right to be forgotten.

As regards the right to deletion, GDPR sets out that in case the data controller has disclosed the personal data (which must be deleted), it is obliged to take reasonable steps to inform other controllers that are processing such data regarding the request of the data subject on deletion thereof. Concerning the right to object the automated decision-making, GDPR has introduced the concept of 'profiling' as part of automated processing. 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. In addition, in this regard, GDPR further stipulates that the data controller is obliged to inform the data subject in explicit terms (i.e. presented clearly and separately from other information) at the latest at the time of first communication with the latter. The same also applies in case of the right to object to direct marketing.

None of the above rights are provided for under the provisions of the Albanian legislation. The spirit of the law might (somehow) imply such rights, but in practice we believe that the data controllers in Albania might not consider them.

6. REGISTRATION OF DATA PROCESSING ACTIVITIES

As already mentioned above, the Current Data Protection Law provides for the obligation of data controllers to notify the Commissioner regarding any processing of personal data for which they are responsible, even before the processing takes place, for the first time or in case of changes to the processing activities.

The notification should contain the prescribed information on a particular data processing (e.g. name and address of the data controller, scope of the data processing, categories of the data subjects, types of the processed data, etc.). It should be made through a notification form which can be completed (in Albanian language) and submitted online to the Commissioner or through a soft copy submitted in person or via courier to the Commissioner's address. A summary of the respective data processing activities is entered in the so-called Central Registry of the Commissioner which is available to the public through the Commissioner's website.

Considering that the GDPR prescribes only the obligation of keeping internal records of data processing activities (and making such records available to supervisory data protection authorities upon their request), rules of the Current Data Protection Law by which the above-described notification (and further registration) of data processing activities is prescribed are not aligned with the GDPR.

7. DATA BREACH RELATED NOTIFICATION AND DATA PROTECTION IMPACT ASSESSMENT

The Current Data Protection Law, as opposed to the GDPR, does not provide explicit rules on data breach notification. The Commissioner has however filled in this gap by prescribing (through its Instruction no. 47 detailed in Section 2, Item 10 below) the obligation of large data controllers to report any serious data security breach to the Commissioner.

According to the Instruction, the DPO shall notify the data processor, in writing and in due time, in relation to each risk of breach of data subject's rights, including infringement of data protection legislation. If after being notified, the data processor fails to take adequate measures to address the breach in due time, the DPO should notify the Commissioner.

The institute of data protection impact assessment is not expressly governed by the Current Data Protection Law either, but to some extent has been aligned with GDPR through instruction no. 47 detailed in Section 2, Item 10 below. In this regard, the Albanian legislation (i.e. Instruction no. 47) obliges all large data controllers to make impact assessment before starting the processing of personal data, however it does not confer onto the Commissioner any room for determining the range of activities that such impact assessment should undergo and, as a result, consulting obligations with the Commissioner.

8. DATA TRANSFER

The Current Data Protection Law allows free international transfer of personal data generally only to the economies which guarantee an adequate protection of personal data, otherwise a prior transfer approval from the Commissioner is required.

The list of economies which guarantee an adequate protection of personal data is provided by Decision of the Council of Ministers no. 934, dated 2 September 2009 "On the determination of the economies which have a sufficient level of personal data protection". According to this Decision, these economies are the members of the EU and the members of the European Economic Area (EEA) and also the economies which have ratified the Strasbourg convention no. 108, dated 28 January 1981 "For the protection of individuals with regard to automatic processing of personal data" and its additional protocol. Hence, the respective economies guarantee a sufficient protection of personal data, in compliance with the Directive 95/46/EC of the European Parliament and Council, dated 24 October 1995 "On the protection of individuals with regard to the processing of personal data and on the free movement of such data". The Decision also includes economies in which personal data can be transferred according to a decision of the European Commission.

The Current Data Protection Law explicitly provides for two exceptions when international transfer of data is allowed even if made to an economy which does not provide adequate protection in the aforementioned sense. The first exception covers the following explicitly prescribed cases: (1) the transfer is authorised by ratified international acts that are directly applicable in Albania, (2) the given consent of the data subject, (3) the international transfer is necessary for the performance of a contract between the data subject and the data controller, for the implementation of pre-contractual measures taken to address the data subject's request or, for the conclusion or performance of a contract between the controller and a third party, in the interest of the data subject, (4) the transfer is a legal obligation of the controller, (5) the international transfer is necessary for protecting vital interests of the data subject, (6) the transfer constitutes a legal requirement over an important public interest or for exercising and protecting a legal right, and (7) the transfer is done from a register that provides information to the general public.

In case none of the above legal grounds is applicable, international data transfer is possible with the prior authorisation of the Commissioner, if the Commissioner is satisfied that adequate safeguards with relation to privacy and other fundamental rights of the data subject are in place. The Commissioner can additionally provide for conditions and obligations under which the data transfer should take place.

The data transfer regime appears not to be fully aligned with the GDPR. While both legal acts set out that as a rule the international transfer can be made to economies with adequate level of personal data protection, as regards the transfer to third economies (i.e. without adequacy decision), the GDPR stipulates that the transfer to such economies is allowed

also in case that appropriate safeguards to such purpose are in place. Except for the use of the Standard Contractual Clauses (i.e. as per the decision of the European Commission reflecting the requirements of the Directive 95/46/EC) for demonstrating that data controller provides adequate level of protection of personal data protection (i.e. when applying for issuance of the authorisation of the Commissioner for international transfer of personal data to economies without adequacy level), the Albanian legislation does not foresee any such safeguards (i.e. Binding Corporate Rules, approved code of conduct, etc.).

Moreover, Albanian legislation freely allows the international transfer of personal data to economies without adequate level of personal data protection in case derogations indicated above apply. Wording of Article 8 of the Current Data Protection Law appears to indicate that the use of such derogations might apply at any time, for any routine transfer to the economies without adequate level of personal data protection although in practice the Commissioner requires that the data controllers should apply for authorisation even in cases when one or more such derogations are in place. While according to GDPR, the decision on transfer of personal data to economies without adequate protection is based on the similar derogations as those of the Albanian legislation, we understand that such transfer is allowed only in specific situations and that the use of such derogations (i.e. such as the consent of the data subject) should not be considered and used on routine international transfers, but should relate solely to specific circumstances applicable to each transfer. Moreover, it appears that GDPR is more careful in respect of derogation related to own consent of the data subject for the purpose of enabling the international transfer to economies without adequacy level, i.e. to this effect, it states that the data controller should inform the data subject of the possible risks that might result due to the lack of an adequacy decision and appropriate safeguards in relation to an international transfer. Such informed consent requirement is not expressly provided in the Current Data Protection Law. In addition, unlike GDPR, the Albanian legislation provides no rules regarding the transfer of personal data to international organisations.

Based on the annual reports of the Commissioner, it can be noted that the Commissioner has authorised several international data transfers in economies that fail to provide a sufficient level of data protection. In other cases, when data was transferred to economies with an adequate data protection in place, authorisation from the Commissioner was not required.

During 2019, for example, the Commissioner handled 16 transfer practices for authorising data transfers in economies with insufficient level of data protection and one decision was issued in this respect to authorise international data transfer in the banking sector. In this decision, the Commissioner stated the categories of data that will be transferred, the data retention period and further emphasised that the data be transferred only to meet the purpose declared in the notification form filed with the Commissioner.

In 2018, the Commissioner authorised 14 international data transfer practices out of which two were related to banking and pharmaceutical sectors.

Generally, if based on the notification forms filed by data controllers the Commissioner detects that data are transferred to economies with insufficient level of data protection, additional information is requested from data controllers and the relevant transfer practices are reviewed by the Commissioner.

Although the number of decisions authorising international data transfers is seemingly low, it does not represent the total number of international data transfers taking place. This is because, in most cases, data is transferred to economies which guarantee an adequate level of protection of personal data, therefore a prior transfer approval from the Commissioner is not required.

9. PENAL POLICY

One of the main differences, among others, between the Current Data Protection Law and the GDPR, is the penal policy. This is due to the fact that, unlike very stringent penal policy and extremely high fines introduced by the GDPR (i.e. fines in the amount of up to EUR 20,000,000 or 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher), the Current Data Protection Law provides for a very mild penal policy.

According to the respective Law, what does not constitute a criminal offence with relation to unlawful data processing will be subject to administrative sanctions and fined under the Current Data Protection Law. Fines vary from 100 000 ALL (approx. EUR 75) up to 1, 000, 000 ALL (approx. EUR 750). The fines are doubled when violations are attributed to legal persons and in case the controller changes the personal data of the data subject after the latter has filed a complaint and a final decision has not been taken yet. The fine is also doubled in the case of processing of personal data without the preliminary authorisation of the Commissioner. However, even when doubled, their values are rather symbolic, in particular when compared with the penal policy introduced by the GDPR. In any case, the fines are imposed by the Commissioner.

10. RELEVANT SECONDARY LEGISLATION

In addition to the Current Data Protection Law, other relevant data protection legislation includes a variety of decisions, instructions, guidelines, recommendations of the Commissioner, etc. Some of the main secondary legislation includes the following Decisions and Instructions of the Commissioner:

1. **Instruction no.47 "On determining rules for safeguarding personal data processed by large controllers" ("Instruction no. 47") and Instruction no.48 as of 2018 "On the certification of systems managing information security, personal data and their protection" ("Instruction no. 48")**

These instructions are described below together as both apply to large data controllers and processors in Albania. According to Instruction no. 47, large controllers include controllers and processors that process personal data manually or electronically, by employing 6 or more persons for the processing, either directly or by virtue of processors.

When it comes to large data controllers, the Commissioner has provided for more stringent rules regarding security of personal data processing and archiving systems, vis-à-vis to those applicable to small data controllers.

In this view, Instruction no. 47 stipulates that all large data controllers/processors are obliged to establish and maintain the Information Security Management System ("**ISMS**") for the protection of personal data. This system is based on the identification, analysis and mitigation of the risks threating the security of personal, by considering the weaknesses of ICT systems used for the processing of personal data, of all manual forms of processing, as well as of the physical security, inside and outside the premises of processing activities, security of personnel and portable electronic devices.

When determining the ISMS for their own activity, the data controllers should consider the standards of information security, such as confidentiality, integrity, availability, and reliability of ICT systems used for personal data processing.

The ISMS comprises, inter alia, an analysis/assessment of the impact that the processing operations might have on the rights and freedoms of data subjects and the applicable Information Security Policy ("**ISP**"). The impact assessment should be conducted prior to the commencement of personal data processing. Through this action, the data controller carries out an assessment of the impact of processing operations in order to identify where such operations would present risks to the rights and freedoms of the data subjects.

The ISP, on the other hand, aims to protect the security of personal data from any risks and breaches that they might be exposed to. The ISP should clearly specify the security objectives and determine the technical, organisational and personnel related security measures in order to mitigate the threats and risks affecting the archiving system. A special focus in this regard should be granted to the processing of sensitive data, management of access right (i.e. which is related to the standard of availability and reliability of ISMS) and risks resulting from the access in the public networks/internet.

Among the others, the ISP should contain a risk assessment and an analysis of the archiving systems (i.e. same as in case of small data controllers described above), as well as the commitment and support of the management of the data controller/processor toward the information security, and detailed regulations on security (i.e. technical, organisational and personnel related measures, manner, form and periodicity of inspection activities, procedures to be followed during system breakdowns and possibilities for an efficient restoration of situation as it was prior to occurrence of system breakdown/security failure, etc.),

The large data controllers are obliged to deliver annual training to the personnel engaged in the processing of personal data. The training should also be delivered in case of any significant amendments to the legislation on personal data protection, significant amendments to the EU framework on personal data protection, changes to ISMS, etc.

As regards the relationship between data controller and data processor, Instruction no. 47 sets out that the data controller is obliged to check the compliance of the data processor with the legislation on personal data protection prior to concluding the outsourcing contract with the latter. To this effect, in case the data controller engages more than one data processor, the latter should have an ISMS in place. In case of engagement of only one data processor, the data controller is obliged to communicate to the latter the applicable parts for the ISMS, which shall be legally binding in the outsourcing contract.

Furthermore, Instruction no. 47 provides also for rules in case of personal data processing through, inter alia, cloud computing.

The ISMS should comply with the legislation in force and recommendations prepared by professional industry organisations/associations, including banks, telecommunications, insurance, social security and health care.

In addition, the ISMS should comply with the technical standards related to the ICT security systems and best practices applicable in the field of information security.

In this view, the entire ISMS should be compliant with the ISO/IEC 27001 and the large data controllers are obliged to perform annual controls of the personal data/information security. To such an end, Instruction no. 48 sets out that such control should be performed by the accredited bodies. In addition to that, the same instrument provides for the certification of conformity of ISMS with the foregoing ISO standard. The certification is done every three years through the accredited bodies.

The accredited bodies should fulfil the criteria set out under Instruction no. 48, which include, inter alia, the accreditation by the national accreditation authority and authorisation of the Commissioner for the purpose of performing the assessment/certification of the ISMS. They will be registered in the registry of accredited bodies held by the Commissioner.

As noted above, Instructions no. 47 and 48 are quite detailed as regards the obligations of data controllers (and processors) to ensure and maintain personal data security. Especially in case of large data controllers, considerable attention is paid to establishment, functioning, management and maintenance of the Information Security Management Systems (ISMS) in compliance with the ISO/IEC 27001.

Hence, as a general note, it might be said that the provisions of the Current Data Protection Law and secondary legislation are generally aligned with the GDPR in respect of the above areas.

GDPR provides that the data controllers are obliged to carry out the impact assessment regarding the processing operations they will carry out. Therefore, the supervisory authorities are obliged to establish and make a public list of processing operations that should undergo the impact assessment procedure. In addition, the data controllers are obliged to consult the supervisory authority in case the impact assessment suggests that the relevant processing operations can result in a high risk in absence of measures to be taken by the controller against such risk.

In this regard, the Albanian legislation (i.e. Instruction no. 47) obliges all large data controllers to make impact assessment before starting the processing of personal data, but the Instruction (or the Current Data Protection Law) does not confer onto the Commissioner any room for determining the range of processing activities that should undergo such impact assessment. As such, no consulting obligations are set out in the Law or Instruction no. 47.

The GDPR provides for the possibility of data controller to undergo certification mechanisms for the purpose of demonstrating compliance with the GDPR provisions (i.e. if the relevant member state law provides for such mechanisms). In this respect, we can admit that the secondary legislation in Albania has already created a legal framework for the establishment of certification mechanisms (i.e. as per Instruction no. 48, in conjunction with Instruction no. 47). To this effect, it is mandatory for all large data controllers to undergo annual inspections (i.e. security controls) by accreditation bodies to demonstrate compliance with the legislation in force; including ISO/IEC 27001. In addition, the accredited bodies certify the respective ISMS of any data controller, if compliant with the forgoing standard, for a period of three years.

Despite the above remarks, it is to be noted that GDPR contains the following instruments/ obligations which are not yet provided in the Albanian legislation:

1. The data controllers are obliged to implement appropriate technical measures, such as pseudonymization and encryption of personal data;
2. The data controllers might adhere to an approved code of conduct, which represents an instrument that might be drawn up by associations (or other bodies) representing categories of data controllers/processors, for the purpose of complying with GDPR, in relation to, but not limited to, the fair and transparent processing, legitimate interest pursued by controllers in specific contexts, the collection of personal data and their pseudonymisation, the exercise of rights of the data subject, international transfer to third economies, etc.

   Data controllers/processors that are not subject to GDPR (for, example Albanian controllers/processors) might also adhere to the codes of conduct in order to provide appropriate safeguards within the framework of international transfer of personal data.

   The final approval of such instrument is to be done by the supervisory authority;
3. Same as in case of codes of conduct, certification mechanisms may be established for the purpose of demonstrating compliance with GDPR (i.e. existence of appropriate safeguards) of data controllers/processors that are not subject to GDPR itself (for example, Albanian controllers/processors) within the framework of international transfer of personal data;
4. The data controllers are obliged to notify the supervisory authority without undue delay (however, not later than 72 hours) in case of a personal data breach.

   The notification should describe the nature of the personal data breach, communicate the name/contact details of the data protection officer or other contact points where more information can be obtained, describe the likely consequences of the personal data breach and the measures taken (or proposed to be taken) by the controller to address the personal data breach.

Moreover, the data controller is obliged to document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. Such documentation should enable the supervisory authority to verify compliance with GDPR.

It is to be noted that, in relation to the notification of the Commissioner regarding the data breaches, the Albanian legislation (Instruction no. 47) provides only for the obligation of the Data Protection Officer to notify the Commissioner of the risks to which the processing activities of the data controller are exposed to, if the latter fails to take the appropriate measures against such risk (despite the warning of the Data Protection Officer).

In addition, the Guideline no. 47 elaborates in detail the requirement regarding appointment of a contact person, i.e. DPO for large data controllers. The details on the DPO are provided in Section 2, Item 3 of Chapter I of this report.

2. **Decision no. 2, dated 10 March 2010 "On determination of administration procedures on registration of data, insertion, processing and extraction of personal data" as amended ("Decision no. 2")**

The Decision no. 2 sets out the rules for (1) administration of data registration, (2) entering of data, (3) processing of data, (4) disclosure and (5) confidentiality of data and applies to all public and private controllers.

Storing and preserving of data: data storing and preserving requires a specific, clearly declared aim for which the data is stored and then processed. In view of this, every person, whose data is being collected, stored and processed has the right to be informed on the reason for the collection and storing of his/her data as well as on the aim of data collection. Every subject possessing data should inform the person whose data he/she is possessing on such administration.

Correct and updated data: the data shall be stored in a correct and timely manner, no longer than necessary for the purpose for which they have been collected and/or processed. The data subject shall be granted all the rights provided under the Current Data Protection Law. To ensure the data is accurate and updated, the general storing requirements shall be considered in full and appropriate procedures must be imposed, applied, and implemented, including periodic review of the data. These procedures should be sufficient to ensure appropriate verifications that guarantee data accuracy.

Clear data storage timeframe: regarding the storing period, data controllers are responsible to determine the timeframe within which data will be stored, as instructed by the Commissioner and have a clear policy in place to ensure that. An appointed person will regularly monitor the databases to ensure that data are not held for longer than necessary.

Access right of data subjects: it is further stated by the Decision no. 2 that every individual, whose data is being stored, is entitled to access such data. By access, the data subject has the right to: (1) be informed on the data being processed; (2) know the data source; (3) be informed on the persons to whom the data has been disclosed, and (4) know the rationale behind automatic decisions.

Data security: to ensure a minimal security standard, the data shall be stored under security standards to prevent unauthorised access. Computer systems should be encrypted and access to data shall be restricted to certain personnel. Other measures include technical arrangements to ensure data protection, destruction of all acts and documents containing unnecessary personal data, appointment of an authorised person to ensure that data are safe and updated, etc.

International transfer of data: In case of international data transfer, a sufficient level of data protection should be ensured. This is in line with Article 45 of GDPR allowing data transfers based on an adequacy decision in relation to the level of data protection provided in the economy where data are to be transferred. Therefore, the category of the data being transferred, the data protection legislation of both the transferring and the recipient economy, specifically provisions applying in relation to data belonging to foreign citizens as well as other measures undertaken by those economies to ensure data protection, need to be considered. The decision authorising the international data transfer shall also consider whether: (1) the data have been used for the purpose of the transfer; (2) the data subject has the right to be informed on the aim of processing of his/her data; (3) the foreign controller applies the same procedure and means for the protection of personal data, etc.

In its second part, Decision no. 2 regulates the entering of data based on Articles 5, 6, 20, 22 and 27 of the Current Data Protection Law. Entering of data, as well as gathering and storing, shall be conducted fairly. In order for data to be collected in a fair way, the data subject should be informed on his/her rights and shall be provided with the relevant information related to the processing of his/her data (i.e. the name of the controlling entity and the purpose of collection). Entering and processing of data shall be the main subject matter of the contract concluded between the controller and the data processor. The contract shall state the conditions and the criteria based on which the data is requested, collected, entered, or processed by the processor, together with other technical conditions regarding data security. The controllers are entitled to take the necessary measures to guarantee the implementation of conditions and criteria provided in the contract.

In relation to the processing of data, the personal data shall be taken in a fair way as consented by the data subject unless based on one of the grounds listed under last paragraph of Section 2, Item 1 of Chapter I of this report. These criteria mentioned under both Decision no.2 and the Current Data Protection Law are aligned with Article 6 of the GDPR with regard to lawfulness of processing, providing for processing to be considered lawful only if and to the extent that at least one of the following applies:

1. The data subject has given consent to the processing of his or her personal data for one or more specific purposes;
2. 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;
3. Processing is necessary for compliance with a legal obligation to which the controller is subject;
4. Processing is necessary in order to protect the vital interests of the data subject or of another natural person;
5. 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;
6. 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.

The same applies to sensitive data, the processing of which should be consented by the data subject, unless processing is based on one of the grounds provided under the second paragraph of Section II 4 of this Report.

These criteria are also mirrored under Article 9 of the GDPR, although the latter provides a more complete regulation about processing of special categories of personal data, i.e. processing is necessary for the establishment, existence, or defence of legal claims. However, if broadly interpreted, provisions of Article 7 of the Current Data Protection Law can justify processing also in other scenarios except for those explicitly mentioned in the

Law, in the name of the vital interests of the data subject (i.e. the defence of legal claims of the data subject). In any case the data should be sufficient and appropriate in relation to the purpose for which data is requested. The same requirement applies for data disclosure, to follow the aim for which the data is collected and/or processed.

The Decision no.2 ends by stating the confidentiality obligation of data controllers, processors and third parties employed by data controllers or processors, prohibiting them to disclose the data they process.

3. **Decision no. 8 "On the economies with an adequate level of protection for personal data", as amended ("Decision no.8")**

Article 8.1 of the Current Data Protection Law allows free international transfer of personal data to economies which guarantee an adequate level of personal data protection.

The list of economies which guarantee an adequate level of protection of personal data is provided by Decision No. 8 of the Commissioner. According to this Decision, these economies are: (a) the EU MS; (b) economies part of the European Economic Area; (c) members that have ratified the Strasbourg Convention No.108 for the Protection of Individuals regarding the automatic processing of personal data and related protocol; and (d) economies designated by a decision of the EU Commission. A list naming all the economies falling under any of the above categories is attached to this decision as Annex 1.

4. **Decision no. 6 "On establishment of detailed rules for personal data security" ("Decision no. 6")**

By means of Decision no. 6, the Commissioner determines specific mandatory rules for public and private controllers in relation to data processing.

Generally speaking, this Decision is in line with what is provided under the GDPR in respect of the obligation of the controller to ensure data safety measures. Article 24.1 on the responsibilities of the controller and Article 32.1 of the GDPR on security of processing, respectively provide the obligation of controllers and processors to implement appropriate technical and organisational measures to ensure that processing is performed in accordance with the Regulation and an adequate level of security is provided. In the same line, Decision no.6 sets out rules for controllers to ensure adequate level of data security and for processing activities to be compliant with the requirements of the Law.

The following constitute the obligations of the controller under Decision no. 6: (1) determine the categories of personal and sensitive data being processed; (2) determine the levels of access to data, in compliance with their job profile, in function of the processing and protection of data; (3) draft and approve a regulation "On the protection, processing, storage and safety of personal data", based on the template draft/regulation provided by the Commissioner; (4) take the necessary steps and ensure that the staff is aware and trained on the need for data safety; (5) draft and implement a privacy policy and rules for the security of access in the premises in which the data processing is performed; (6) ensure that every employee engaged in data processing has agreed to a "confidentiality agreement" as per the template annexed to the Decision; (7) draft and implement procedures to keep record of possible modifications, destructions and transfers of data during their processing, etc.

Failure to fulfil the above obligations is considered a breach of the Current Data Protection Law.

5. **Decision no. 4 "On determination of exceptions from the obligation to notify the processing of personal data" ("Decision no. 4")**

As provided under Article 21 of the Current Data Protection Law, every data controller shall notify the Commissioner about the processing of personal data for which it is responsible.

However, paragraph 4 of the same Article allows the Commissioner to determine specific cases in which notification is not necessary. Decision no.4 of the Commissioner provides that the processing of personal data should not be notified to the Commissioner in case: (a) processing is performed by non-profit organisations, political organisations, trade unions, religious or philosophical organisations for the purposes of their legal activity, for members, sponsors or other persons continuously related to the activity of these organisations; (b) processing of data concerning the management of human resources in the public and private sector, in the exercise of the legal rights and obligations, if the processing is limited to: the purpose of job admission; applications; competitions; appointments; removal from duty; qualifications; calculation of salaries; etc. However, in case the data being processed in this latter case is considered sensitive, the processing notification is mandatory; and (c) processing is performed under Law no.9154 as of 06 November 2003 "On archives" but is limited to the fulfilment of the necessary purposes in accordance with the Current Data Protection Law.

Recital 89 of the GDPR provides that the obligation to notify processing to the Commissioner no longer exists as it was abolished with the repeal of Directive 95/46 EC considering this obligation provided administrative and financial burdens for the controllers and not always contributed to improving the protection of personal data.

6. **Instruction no. 19 "On regulation of the relationship between the controller and the processor in case of delegation of personal data processing and master contract form for such legal arrangements" ("Instruction no. 19")**

Pursuant to Article 30.1(c) and Article 31.1 of the Current Data Protection Law, controllers can delegate the processing of personal data to processors in which view this instruction regulates the relationship between the data controllers and data processors. All controllers entering a contractual relationship with a third-party company for processing of personal data are bound by this Instruction, the non-application of which is punishable accordingly the Current Data Protection Law.

All companies, organisations or institutions, which, while performing their duties, enter into relationships with third party companies, either foreign or Albanian, and agree for the latter to process data on their behalf by means of a written contract, shall be bound by this Instruction and draft a contract to regulate the relationship in accordance with the legislation. A contract sample is annexed to the Instruction. The contract shall define the rules for processing of personal data as well as the measures to be taken by the data processor to ensure sufficient protection of data as well as the steps to be taken in case of a breach. The controllers are required to assure a good selection of the processor as the latter should ensure appropriate protective measures for the data they will process. Article 28.1 of GDPR provides the same obligation, through an extended language, requiring the processor to provide sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

In respect of data protection, the data controller and data processor can either draft a special contract for establishing data protection rules or include those rules as part of the main business contract. The contract should clearly state that the processor uses and discloses data as instructed by the controller and guarantees that it is able to provide an adequate level of data protection. Moreover, the outsourcing contract should regulate the cases when the processor shall notify the controller of any possible damages caused to the data subject or to the data controller in case the damage is related to the controller's business position and reputation.

With the approval of the controller, the processor itself can enter a contract with another company, (i.e. a subcontractor) that is also subject to the same appropriate safety rules applicable for data processors as provided hereinabove.

7. **Guidance "On processing of sensitive data and obtaining of authorisations"**

This guidance offers some basic recommendations for public and private controllers and processors in relation to the processing of sensitive data, to ensure application of the data protection legislation. Sensitive data are defined, according to the Current Data Protection Law, as data in relation to a person's:

1. Ethnical and racial origin;
2. Political views;
3. Trade union memberships;
4. Religious or political beliefs;
5. Criminal charges and
6. Health and sexual life.

The Guidance, as opposed to the Current Data Protection Law, is aligned with the GDPR in the sense that it also considers as sensitive unique biological features such as biometric data, fingerprints, retinal images, genetic characteristics, etc.

The Guidance further elaborates on the meaning of public interest in the context of restriction of data subject rights as noted above. While there is no exhaustive definition of public interest, the circumstances that define public interest include: national safety; territorial integrity and public security; prevention of crime and terrorism; protection of health and moral; protection of the reputation or the rights of other individuals, etc. In view of this, the legal rights and interests of natural and/or legal persons can be restricted proportionally to the prevailing public interest and in accordance with the law. The Commissioner shall authorise controllers for processing of personal data when necessary to protect an important public interest. Before processing of sensitive data, in the request for authorisation filed with the Commissioner, controllers should provide complete information with regard to the controller (information on the object of his/her activity; his/her location, etc.); the purpose(s) of processing of sensitive data; the recipient and the category of recipients of sensitive data; the means and the way sensitive data is processed; the persons having access to the sensitive data, etc. After assessing the full application, the Commissioner will evaluate on whether the processing of sensitive data is necessary in the name of public interest, and if so, further authorise the processing.

The safety measures in place, when processing sensitive data, require the data controller to: (1) respect the data subject's rights with regard to privacy and (2) inform the data subject on the processing of his/her sensitive data and on third parties that have access to his/her data; (3) ensure the purpose for which sensitive data are being processed is clear and lawful; (4) appoint responsible persons to supervise that processing of sensitive data is performed according to the law and draft specific rules applicable to them; (5) clearly identify the persons who have access to a person's sensitive data, etc. Furthermore, processing of sensitive data shall only be performed by authorised persons who, because of their duty, collect, process and store sensitive data in areas such as healthcare; insurance; judicial system; administrative agencies; etc. As regards employees of the public sector, controllers will only provide them access to what is necessary to provide the service to the data subject.

Measures in place for the processing of sensitive personal data not only include adequate hardware and software systems in place (i.e. systems to detect access and processing of sensitive data, auditing systems to control access on database and detect possible abnormalities, etc.), but further require for organisational measures such as periodic training of the personnel on the safety rules and standards of sensitive data; determination of additional, specific procedures for handling of documents in writing in view of preventing access of unauthorised persons to sensitive data; usage of personal data only in accordance with the provided authorisations of responsible persons and in compliance with legal provision on processing of personal data; etc. In conclusion, the Guidance offers a general overview about processing of sensitive data and the procedures to be followed by the controller prior to processing activities.

8. **Guidance "On determination of Data Controllers who are obliged to notify the Commissioner on processing of the personal data for which they are responsible"**

As its name indicates, this Guidance aims to determine data controllers that are obliged to notify the Commissioner on processing of personal data for which they are responsible. The notification is not only required the first time that controllers start to process personal data but also when changes to the notified processing activities take place. Data controllers, data processors and third parties have the same meaning as defined under Article 3 of the Current Data Protection Law, respectively:

"Controller" shall mean the natural or legal person, public authority, agency or any other body, which alone or jointly with others determines the purposes and means of processing of personal data, in compliance with the laws and secondary legal acts applicable, and who is responsible for the fulfilment of obligations defined by the law.

"Processor" shall mean a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the Controller.

"Third party" shall mean any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorised to process the data.

As stated under Article 21.1 of the Current Data Protection Law, data controllers are required to notify the processing of personal data for which they are responsible to the Commissioner either online, by electronically submitting the filled notification form through the official website of the Commissioner (www.idp.al), or by filing the notification form physically or by post with the Commissioner. The information provided in the notification forms is published on the official website of the Commissioner under the publicly available Electronic Register of Controllers, accessible at www.idp.al. This provision is similar to what is provided under Article 30 of GDPR on records of processing activities although the latter states for the obligation of each controller to maintain a record of processing activities under its responsibility other than notifying the processing with the Commissioner as provided under both Article 21 of the Current Data Protection Law and this Guidance. The latter obligation is abolished and is no longer present in the GDPR. However, upon the request of the supervisory authority, as stated under Article 30.4 of GDPR, the controller and the processor (as he/she shall also maintain a record of processing activities carried out on behalf of the controller) shall make the records available.

Data controllers that are obliged to file a notification with the Commissioner are all public or private subjects who define the purpose related to the way in which personal data is processed. Controllers in the public sector include the Council of Ministers; the Parliament; constitutional and other independent institutions established by specific law; general directories; ministries and dependent institutions; prefectures, diplomatic missions abroad; armed forces; municipalities; commercial companies with private or public capital which have been delegated to offer public services; etc. Controllers in the public sector will be considered as such only in case they are entitled to determine the purpose of processing in relation to the way in which processing is performed, otherwise they will be considered as processers. Controllers in the private sector are natural or legal persons, profitable or not, that collect and administer personal data by determining the purpose in relation to the way in which data is processed and are therefore obliged to notify the Commissioner for the first time and in case a change of processing notice status is required. The same applies to controllers in the private sector that are not located in Albania but perform their activity by using means located in Albania.

Private entities established as branches of large data controllers that do not determine the purpose in relation to the way in which data is processed, but only enforce the obligations as determined by the mother company, are not considered data controllers and are not obliged to notify the Commissioner.

Controllers exempted from the obligation to inform the Commissioner on the processing of personal data are obliged to provide the following information: (1) name and address; (2) the category of the personal data processed; (3) the purpose of processing of data and (4) the category of recipients. They are however obliged to notify the Commissioner in case of international data transfer by using one of the methods explained above. The Guidance is concluded with a disclaimer that in any case controllers that are obliged to notify data processing to the Commissioner will be assessed on a case-by-case basis.

3. COMPETENCE OF AND CHALLENGES IN THE WORK OF THE COMMISSIONER

The public authority with the competence in the field of data protection is the Commissioner for the Right to Information and Protection of Personal Data (in Albanian, Komisionieri per te Drejten e Informimit dhe Mbrojtjen e te Dhenave Personale).

According to the Current Data Protection Law, the Commissioner is a public legal entity and independent authority in charge of supervising and monitoring the protection of personal data and the right to information by respecting and guaranteeing the fundamental human rights and freedoms in compliance with the law.

However, it is not a self-financed institution in the meaning of the law. The budget of the Commissioner is funded by the government budget and donors that do not manifest any conflict of interest. Detailed information on how the budget is spent is published on the official website of the Commissioner. The Commissioner is elected by the Parliament, upon a proposal of the Council of Ministers for a term of 5 years. His/her function is incompatible with any other government function or affiliation in political parties as well as any other profitable activity except for teaching. The Commissioner is obliged to prepare an annual report on its activities that is submitted to the Albanian Parliament.

There are no other authorities in Albania that are directly responsible for the supervision and enforcement of data protection legislation other than some limited sectoral regulation provided, for example, in the electronic communications legislation only in respect of data breaches[2].

The Commissioner, according to the Current Data Protection Law, has the right to: (1) conduct an administrative investigation, have access to personal data processing and collect all necessary information with the view of fulfilling his supervisory obligations, (2) order for the blocking, deletion, destruction or suspension of the unlawful processing of personal data, (3) issue instructions prior to the data processing and ensure their publication. In cases of recurring or intentional serious infringement of the Current Data Protection Law by a controller or processor, especially in cases of recurring failure to implement the Commissioner's recommendations given to a controller/processor, the Commissioner can impose the fines provided in the Current Data Protection Law.

2 According to the electronic communications law, a data breach notification is considered to be mandatory for the provider of publicly available electronic communications services who must notify the breach without undue delay to the Electronic and Postal Communications Authority and not the IDP. If the personal data breach is likely to be detrimental to the personal data or privacy of the contracting party or another individual, the electronic communications provider should also notify the contracting party or the individual without delay. Notification will not be required if the provider has demonstrated to AKEP that it has implemented the technical protection measures that render the data unintelligible to any entity that is not authorised to access it.

Some of the concrete competences of the Commissioner provided in the Current Data Protection Law include:

1. Providing opinions on draft legal and secondary acts related to personal data;
2. Providing recommendations for the implementation of the obligations deriving from the law on protection of personal data and ensuring publication thereof;
3. Authorising in special cases the use of personal data for purposes not designated during the phase of their collection by observing the data protection principles provided in the law;
4. Authorising the international transfer of personal data,
5. Issuing guidelines that regulate the length of retention of personal data according to their purpose in the activity of specific sectors;
6. Ensuring the right to information of data subjects and their right to rectify and update personal data;
7. Authorising the use of sensitive data in compliance with the law;
8. Monitoring that processing of personal data by controllers/processors is done in conformity with the law, either ex *officio* or upon request of a data subject;
9. Addressing complaints of data subjects;
10. Issuing guidelines on security measures in the activity of specific sectors;
11. Imposing and overseeing the enforcement of penalties.

One of the main challenges of the Commissioner today is the alignment of the data protection legislation in force with the acquis communautaire which remains a top priority of the authority. With the entry into force of the Regulation 2016/679 and Directive 2016/680, as well as the modernisation of the Convention 108, the Commissioner aims to adopt a new law on personal data protection in the fourth quarter of 2021.

As noted in this report, the Current Data Protection Law fails to adequately address the novelties that the GDPR brought about in the field of data protection. Some of the main changes that are not addressed by the current legislation include (1) lack of location data or an online identifier in the categories of personal data, (2) express lack of genetic or biometric data in the categories of sensitive data in the Current Data Protection Law, (3) lack of the data subject's rights to be forgotten and data portability, (4) lack of specific requirements on data breach notification and data impact assessment, (5) lack of strengthened accountability obligations for both controllers and processors, (6) lack of detailed and practical aspects on giving of consent, etc.

Further, as already noted above, one of the greatest differences between the Current Data Protection Law and GDPR is related to the penal policy. While the GDPR introduced high fines amounting up to EUR 20,000,000 or 4% of the total worldwide annual turnover of the preceding financial year, the Current Data Protection Law provides for a very mild policy that does not truly prompt the private and public sector to stay vigilant and compliant when it comes to enforcement of data protection obligations.

In respect of the above, it should be noted that the Commissioner is a beneficiary of the EU 2017 IPA twinning project "Institution Building for Alignment with EU Acquis to Meet Economic Criteria Related to Data Protection" that aims to approximate the Albanian legislation with that of the European Union, more specifically with the GDPR and the Police Directive 2016/680. In this respect, in 2019, the Commissioner's Office carried out all the preparatory work for the implementation of the project which is now expected to start. The project will consist of the review of the Current Data Protection Law or approval of a new

law altogether and the review and amendment of all secondary legislation approved under the Current Data Protection Law.

Another important challenge of the Commissioner based on its 2019 Annual Report remains its understaffed institutional capacity. The Commissioner's office comprises 37 employees responsible for enforcement of both data protection and information rights legislation.

This structure, while sustainable, needs additional resources to cover all the activities of the Commissioner, an issue which has been highlighted continuously also in the annual progress reports of the European Commission for Albania.

One of the most recent challenges in the work of the Commissioner was related to supervision of data processing activities during the Covid-19 pandemic. Despite the Covid-19 outbreak in Albania in March 2020, the Commissioner remained active in performing its duties and obligations stipulated by the law. In the last 6 months, the Commissioner issued several guidelines addressing mainly data controllers' activity during the pandemic, summarised as follows:

1. Guideline on the protection of personal data in the context of the measures taken against COVID-19 as of 20 March 2020;
2. Guideline on the processing of personal data in specific sectors in the context of measures against COVID-19.

   This guideline deals with processing of personal data for Covid-19 purposes in employment, telecommunication, health and education areas:

   - Regarding processing of personal data of employees: Employers who have required the presence of their employees in the regular workplace, in addition to ensuring hygiene and sanitary measures, shall constantly monitor their employees' health conditions so as to prevent the spread of COVID-19. In case of employees working from home, they can access their employers' platforms through virtual private networks (VPNs), or use private communication channels (such as personal e-mail addresses), etc. In such case, the Commissioner's Office considers that employers may, in principle, process their employees' personal data (e.g. data obtained from the elevated tracking of their health) in quantity and quality which – reasonably – would exceed the normal processing of data under a normal working context. Processing involves not only the collection and storage of processed health-related data, but also the transmission of the latter to competent bodies in charge of surveilling the pandemic (as provided by the legislation on the prevention of infectious diseases). Employers should not process personal data beyond what is necessary in relation to the purpose of implementing measures against Covid-19 and for as long as necessary and adequate to achieve the purpose in question. Data controllers are required to minimise any possible risk generated by the processing of personal/ health data, in particular the risks threatening human dignity and privacy;
   - Transmission of location data processed in electronic communication services: As one of the main responses to the pandemic, contact tracing, through the transmission of the individuals' location collected by electronic communications service providers, requested the attention of the Commissioner. The Commissioner's Office, in line with the position adopted in the EU, recommends that before communicating location data, the electronic communications system providers must carry out an assessment of the impact that this type of processing has on the private lives of citizens with the view to strike the right balance between the need for processing location data in the context of Covid-19 on one hand, and the protection of data on the other. The Commissioner considers that transmission of location data performed in an aggregated and anonymous fashion, aimed, for example, to trace movements of infected individuals, does not constitute a violation of the DPL provisions. However, such data processing can only be performed in case the potential benefits deriving to the public health override the benefits of other alternative, less intrusive solutions. In any case, processing of data should be carried out in compliance with the processing criteria set out under Articles 5 and 6 of the Current Data Protection Law and sectorial legislation;
   - Data processing in the context of epidemic surveillance: Events such as the spread of Covid-19 require for special control and tracing measures as approved by the competent authorities for implementing measures in fight of Covid-19. These authorities are also authorised to process personal data, particularly health-related data. Their processing includes collection, storage, and exchange/ transmission of these data to other public and private controllers or competent bodies. Moreover, authorities engaged in the fight against Covid-19 may have an obligation to transfer data to various economies (internationally), and in this context such data transfer should only take place in accordance with the relevant articles of the Current Data Protection Law on international data transfer (Articles 8 and 9 of the Law respectively) and other relevant provisions setting out the legal criteria for processing of personal and sensitive data, i.e. Article 5, Article 6 and Article 7 of the Law;
   - Data processing in the education sector: This section of the guideline deals with universities and lower education institutions that have carried on teaching through online platforms where personal data (including images) of students, pupils, teachers and professors are processed. Processing of personal data in the education sector must be carried out in accordance with the provisions set out in the data protection legislation, i.e. Article 5 of the Law on processing criteria and those of the education sector. The usage of applications and software to ensure continuity of the educational process should not infringe the rights of data subjects and should not be used to process more data than necessary for the legitimate purpose. The Commissioner encourages data controllers to obtain the parents' approval for the intended data processing in the context of online teaching/ learning. Parents and/or custodians should be offered exhaustive information about all aspects related to processing of their children's data, in compliance with Article 18 of the Current Data Protection Law on the obligation of data controllers and data processors to inform subjects whose data they are collecting;
3. Guideline on processing of personal data in accordance with the Covide-19 Hygiene and Sanitary Protocols.

   This Guideline is conceived in the form of Q&A and it addresses concerns of employers, employees, costumers, etc., regarding the rights and obligations in respect of processing activities carried out based on the relevant hygiene and sanitary protocols adopted by the Government.

   According to this Guideline, persons in charge of implementation of the measures specified in the respective Protocols, including record keeping of Covid-19 symptoms, must sign a confidentiality statement on the processing of personal data. In case the employees will be homeworking during the pandemic, due considerations must be given to the use of various online communication platforms to prevent unauthorised access to personal data. Employers must put in place appropriate technical and organisational measures to ensure the security and confidentiality of personal data regardless of whether staff members use personal communication equipment, or those provided by the employer, as the rate of violation of private life as a result of unauthorised processing of personal data when homeworking is greater when compared to working in normal circumstances.

4. CHALLENGES IN THE IMPLEMENTATION OF THE CURRENT DATA PROTECTION LAW IN PRIVATE AND PUBLIC SECTOR

As mentioned above in the introductory part of this report, the challenges currently existing in the field of data protection law in Albania concern both the Commissioner and Local Processing Entities.

When it comes to the Commissioner, the main challenges based on its 2019 Annual Report remain the following ones:

1. Full alignment of the local data protection legislation with the GDPR, and
2. Understaffed institutional capacity of the Commissioner.

As already mentioned in Section 3 of Chapter I herein, according to its 2019 Annual Report the Commissioner's office comprises 37 employees responsible for enforcement of both data protection and information rights legislation. Although this structure is sustainable, from our discussions with the Commissioner we understand that additional resources are needed for the sake of covering all activities of the Commissioner and especially for enforcing its supervision/inspection powers. This is an issue which has also been highlighted continuously in the annual progress reports of the European Commission for Albania as well.

On the other hand, challenges faced by the Local Processing Entities, in both private and public sector, are numerous. They include the following main concerns:

1. Low level of awareness in respect of compliance with the data protection legislation. This refers also to the Local Processing Entities that are already familiar with the data protection legislation's requirements,
2. Lack of knowledge/capacity to assess their current state of data handling procedures, designing and defining new procedures, implementing and administering changes required in the procedures, implementing technologies for the safe processing of personal data, etc.

Specifically, while multinationals present in Albania or domestic tech companies are more familiar with obligations stemming from the data protection legislation and GDPR, there are many other small or mid-size private sector companies in Albania or public sector institutions that are not familiar at all with obligations resulting from their data processing activities, despite several awareness campaigns organised by the Commissioner in this respect.

This can be partially explained by the very mild penal policy provided in the Current Data Protection Law and the fact that, before imposing any fines, the Commissioner tends to issue recommendations to infringing entities to redress the infringement within a specific timeframe.

Once the new data protection law, aligned with the GDPR, enters into force, it will become even more difficult for private and public sector entities to correctly enforce data protection legislation given that proper implementation of new principles, such as accountability, requires them not only to be compliant with the law, but also be able at any time to document and prove their compliance.

For the sake of creating a compliant environment in respect of the existing and future data protection legislation, the following steps should be undertaken as priority:

1. Adoption of the new data protection law fully aligned with the GDPR and harmonisation of all related legislation and sector laws with the GDPR aligned data protection law ("**Full Compliance of the Legislation with the GDPR**");
2. Intensification of the Commissioner's supervision powers by allocating more budget and staff to the Commissioner ("**Intensification of the Supervision**");
3. Public awareness and advocacy of the data protection importance (in particular when it comes to the rights data subjects have under the data protection law) should be further raised ("**Raising Public Awareness and Advocacy**");
4. Strengthening the role of the data protection officer (DPO) as an important tool to guarantee the proper implementation of the data protection legislation in both private and public sector ("**Strengthening the DPO's Role**");
5. Offence proceedings should be initiated without exception against data controllers/processors breaching the law ("**Offence Proceedings**");
6. The Commissioner should undertake training with private and public sector to prepare them for the possible GDPR enforcement in Albania due to its extraterritorial effect and also to familiarise them with the upcoming changes to the Current Data Protection Law and how these will affect their current data processing activities ("**Relevant Data Protection Training**").

Further details concerning each of the above-identified steps follow right below in Section 5 of this Chapter I herein, whereas enumeration of the respective steps should not be understood as the exhaustive list, but only as the list of the most important ones.

5. CRUCIAL STEPS FOR OVERCOMING THE EXISTING CHALLENGES

For the sake of creating a compliant environment in respect of the existing and future data protection legislation, the list of steps of crucial importance, along with the description of each of them, follows below.

I. FULL COMPLIANCE OF THE LEGISLATION WITH THE GDPR

The GDPR, which came into effect on 25 May 2018, repealed the Directive 95/46/EC, therefore, the current Albanian data protection framework is aligned with the respective repealed legal act in the EU.

To date, the Commissioner has made several partial interventions to the legal framework by enacting secondary legislation that is approximated with the GDPR.

In respect of achieving the full alignment of the legal framework with the GDPR, it should be noted that the Commissioner is beneficiary of the 2017 IPA programme of the European Union, i.e. of the twinning project "Institution Building for Alignment with EU Acquis to Meet Economic Criteria Related to Data Protection" that aims at approximating the Albanian legislation with the European Union legislation, more specifically with the GDPR and the Police Directive 2016/680.

In this respect, in 2019, the Commissioner's Office carried out all the preparatory work for the implementation of the project which, according to the discussions with the Commissioner, has finally started at the beginning of October 2020, as already mentioned in the introductory part of this report.

The respective project will consist of the review of the Current Data Protection Law or approval of a new law altogether and the review and amendment of all secondary legislation approved under the Current Data Protection Law. It is also worth mentioning that implementation of this project will be assisted by the consortium comprised of the data protection authority of Italy and Austrian institution Ludwig Boltzmann Gesellschaft.

II. INTENSIFICATION OF THE SUPERVISION

In its Annual Report 2019, the Commissioner emphasised the need of the authority for more capacities, especially in respect of enforcement of its inspection/supervision powers.

At the moment, the Commissioner's office comprises 37 employees in total. This number includes both the employees responsible for data protection matters and employees responsible for information rights legislation. Considering that the respective dual competence of the Commissioner requires significant engagement, there is no doubt that additional resources are needed when data protection matters are concerned in general, and, consequently, as regards Commissioner's inspection authorisations as well.

This objective should be achieved by allocating more budget and staff to the Commissioner. In fact, the GDPR demands higher standards of protection for personal data collected and processed by all types of organisations and the role of the Commissioner is to monitor the application of, and enforce the GDPR.

Additional resources, in particular in respect of IT expertise, will build the Commissioner's investigative capacities and strengthen the Commissioner's technology team to ensure that the office is capable to regulate the use of personal data in emerging technologies.

III. RAISING PUBLIC AWARENESS AND ADVOCACY

In the Annual Work Programme for 2019, the Commissioner considered that raising public awareness on the impact of the GDPR of the Local Processing Entities in both public and private sectors should precede the actual adoption of the new GDPR aligned law.

For this reason, the Commissioner had planned, as included in the Strategy Statement for the period 2018–2020, to undertake the following activities:

1. Organise roundtables and meetings with the Local Processing Entities from private sector by grouping them into specific sectors;
2. Organise training which will focus on the new human resources that should engage in the role of the data protection officer (DPO);
3. Raise media awareness, including social media;
4. Publication of brochures, commentaries and manuals on the innovations of the new data protection law, aligned with the GDPR.

As a general remark, overall transparency and proactive approach of the Commissioner are of crucial importance not only for raising the level of public awareness and further education of the public, but also for strengthening trust of the public in the institution of the Commissioner itself.

IV. STRENGTHENING THE DPO'S ROLE

Once the new data protection law, aligned with the GDPR, enters into force, the data protection officer (DPO) shall be responsible for helping an organisation to ensure compliance with such new legislation.

The primary responsibility of the DPO shall be to make sure that a proper GDPR compliant strategy including policies, processes and procedures is in place across an organisation.

In the light of the above, in the Annual Reports for 2018 and 2019, the Commissioner confirmed that the role of the DPO is a crucial element in respect of the GDPR's implementation. In this respect, the Commissioner has taken a series of measures in order to strengthen the role of the DPO by organising several activities and trainings with such scope.

In this regard, it should, nevertheless, be noted that, under the applicable data protection legislation, the DPO's position can be held only by a person having adequate qualifications.

For the sake of completeness, the main legal criteria to be met by the respective contact person for data protection matters are: to (1) have full legal capacity to act, (2) enjoy integrity, (3) have an university degree in law or computer sciences, (4) be known for professional skills, ethical and moral pure figure, (5) have a working experience of not less than 5 years as a lawyer or IT expert, or has worked for more than 3 years in the Commissioner's office in the position of a lawyer or IT expert, and (6) has not been previously convicted of a criminal offence.

From the perspective of the Local Processing Entities, this means that they/vast majority of them would most probably need to ensure (additional) resources for hiring qualified personnel. It should also be noted that the DPOs, once appointed, should have independence in their work on the data processing matters relevant for the Local Processing Entities which have engaged them.

V. OFFENCE PROCEEDINGS

Based on the current practice, it is not typical that the Commissioner imposes monetary sanctions to public authorities. In fact, there are almost no cases when the Commissioner has addressed breaches of the public and government authorities through monetary sanctions. In case the Commissioner finds breaches in public administration, the normal course of conduct for the Commissioner is to draft recommendation for the respective government body/authority.

For this reason, the crucial change which should happen is that offence proceedings are commenced and conducted whenever breaches of the law occur (and are not cured) regardless whether they occur in private or public sector.

VI. RELEVANT DATA PROTECTION TRAINING

Based on the Strategy Statement for 2018-2020, the Commissioner has considered the important need to train its staff regarding the new upcoming changes to the Current Data Protection law, its legal effects and concrete measures undertaken in practice by the EU counterpart authorities.

Further, the Commissioner has also considered opportune the development of training activities through TAIEX instrument, study visits at the authorities which have implemented the GDPR, signing mutual cooperation agreements and organising activities of common interest (inspection, information and awareness) and exchanging experiences and best practices.

In addition, in the framework of implementing the GDPR in Albania, the Commissioner has performed/participated in various training sessions with foreign experts for the purpose of enriching its staff knowledge and know-how as follows:

1. Data Protection Officer and Codes of Conduct according to the General Data Protection Regulation (GDPR);
2. Training sessions in cooperation with the Albanian School of Public Administration, with the aim on focusing on the rights and obligations of the DPO in the public sector, as well as highlighting the innovations introduced by the enforcement of the new law to be aligned with the GDPR;
3. The Commissioner held the side-event Data Protection in Digital Economy: Third Economies vis-à-vis the GDPR at the Centre for Openness and Dialogue, with aim to establish a dialogue on raising awareness and enhancing possible solutions in achieving GDPR compliance at the level of national legislation;
4. Transparency aspects in the GDPR, organised in the frame of the Albania-EU Anti-Corruption Twinning Project;

5. Institution Building for Alignment with EU Acquis to Meet Economic Criteria Related to Data Protection, aimed at approximating Albanian legislation with that of the European Union, more specifically with the GDPR;
6. Rules on Personal Data Protection in the Health Care System, aimed at raising awareness of the Local Processing Entities in both private and public sector regarding the new rules imposed by the EU upon entry in force of the GDPR.

As a general remark, this type of Commissioner's activities, both towards further education of its staff (but the staff of other government authorities/public institutions as well) and towards the Local Data Processing Entities should be carried out regularly and consistently. The newest developments in the field of data protection law should be regularly monitored and cooperation with the relevant authorities in the European Union, but in the region as well, should be established and/or further developed.

CHAPTER II. BOSNIA AND HERZEGOVINA

1. CURRENT STATUS

The main law governing data protection and privacy in Bosnia and Herzegovina ("**BiH**") is the Law on Protection of Personal Data (Official Gazette of BiH, nos. 49/06, 76/11 and 89/11) ("**Current Data Protection Law**"). The Current Data Protection Law originates from 2006 and was modelled on the EU Directive 95/46/EC and, as such, it is not a GDPR compliant law.

The Current Data Protection Law has significant deficiencies, such as in the field of:

1. Data transfer regime - pursuant to the Current Data Protection Law, adequacy of safeguards for data transfer is evaluated on the basis of specific characteristics of each particular transfer, such as the types of personal data, purpose and period of the processing, economy to which data is to be transferred, statutory rules in force in the respective economy and other relevant circumstances. Furthermore, personal data may be transferred to an economy which does not provide adequate safeguards in the aforementioned sense, in specific cases envisaged by the Current Data Protection Law or with the approval of the Agency in case none of the specific cases are applicable;
2. Legal grounds for data processing - in case of processing for the purpose of protection of the vital interests of the data subject, the Current Data Protection Law, unlike the GDPR, foresees the obligation of the controller to obtain the data subject's consent without delay or to terminate the processing and destroy the collected data. Furthermore, the necessity for implementation of legitimate activities of political parties, movements, civic associations, trade union organisations and religious communities has been recognised as legal grounds for the general data processing Current Data Protection Law prescribes unlike the GDPR which does not recognise the aforementioned as legal grounds for data processing;
3. Rules on video surveillance - the information collected by video surveillance qualifies as personal data due to the fact that the collected information can be used to identify an individual either directly or indirectly by combining it with other pieces of information. Significant implementation of these technologies may limit the possibilities of anonymous movement and anonymous use of services. Even though the data subject might be comfortable with video surveillance set up for a certain security purpose, all precaution measures need to be taken to avoid any misuse of such technologies. The Current Data Protection Law lacks adequate measures that will guarantee avoidance of any misuse of video surveillance;
4. Penal policy - represents the most significant difference between the Current Data Protection Law and the GDPR. Pursuant to the Current Data Protection Law the highest amount of the fine for such breaches is BAM 100,000 (approx. up to EUR 50,000) for a legal entity and BAM 15,000 (approx. up to EUR 7,000) for a legal entity's representative or a natural person, per offence. The GDPR introduced fines in the amount of up to EUR 20,000,000 or 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher, which represents very stringent penal policy and extremely high fines in comparison to the Current Data Protection Law that has a very mild penal policy.

Furthermore, the Current Data Protection Law lacks several solutions/institutes foreseen by the GDPR such as:

- the right to data portability – stipulated by Article 20 of the GDPR pursuant to which the data subject has 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 the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

- the processing is based on consent or on a contract; and
- the processing is carried out by automated means.

In exercising his or her right to data portability, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

- data breach notification – stipulated by Article 33 of the GDPR pursuant to which, 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 supervisory authority, 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 supervisory authority 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. The notification shall:
  - describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
  - communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
  - describe the likely consequences of the personal data breach;
  - describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

  Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.
- data protection officer – stipulated by Article 37 of the GDPR pursuant to which the controller and the processor shall designate 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;
  - 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; or
  - the core activities of the controller or the processor consist of processing on a large scale of special categories of data or personal data relating to criminal convictions and offences.

  The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the following tasks referred to in Article 39 of the GDPR:
  - to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to the GDPR and to other European Union or Member State data protection provisions;
  - to monitor compliance with the GDPR, with other European Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
  - to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35 of the GDPR;
  - to cooperate with the supervisory authority;
  - to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36 of the GDPR, and to consult, where appropriate, with regard to any other matter;
  - to have due regard to the risk associated with processing operations, considering the nature, scope, context and purposes of processing.
- explicit rules on extraterritorial effect – stipulated by Article 3 of the GDRP pursuant to which the GDPR applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the European Union or not.

  The GDPR applies to the processing of personal data of data subjects who are in the European Union by a controller or processor not established in the European Union, where the processing activities are related to:
  - the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
  - the monitoring of their behaviour as far as their behaviour takes place within the European Union.

  The GDPR applies to the processing of personal data by a controller not established in the European Union, but in a place where Member State law applies by virtue of public international law.
- data protection impact assessment – stipulated by Article 35 of the GDPR pursuant to which a type of processing in particular using new technologies, and considering 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, 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 referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or
  - a systematic monitoring of a publicly accessible area on a large scale.

  The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection

impact assessment. The supervisory authority shall communicate those lists to the European Data Protection Board referred to in Article 68, which is composed of the head of one supervisory authority of each Member State and of the European Data Protection Supervisor, or their respective representatives.

The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. The supervisory authority shall communicate those lists to the European Data Protection Board.

Prior to the adoption of the lists, the competent supervisory authority shall apply the consistency mechanism referred to in Article 63 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the European Union.

The assessment shall contain at least the following:

- a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
- an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- an assessment of the risks to the rights and freedoms of data subjects; and
- the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR considering the rights and legitimate interests of data subjects and other persons concerned.

Therefore, having in mind the above elaborated deficiencies and non-alignment with the GDPR, in 2018, the competent authorities initiated the procedure for adoption of a new GDPR compliant data protection law in BiH. Specifically, the draft of the new data protection law ("**Draft Data Protection Law**") was prepared by an interdisciplinary group formed by the members of the BiH Ministry of Justice, BIH Ministry of Civil Affairs, BiH Directorate for European Integration and BiH Data Protection Agency.

According to the publicly available information, the Draft Data Protection Law was forwarded to the BiH Ministry of Civil Affairs at the end of 2018 and the respective ministry should have initiated the adoption procedure before the BiH Parliament.

However, following the elections in 2018, the BiH Parliament was formed with almost a two-year delay, after which the Covid-19 pandemic followed, due to which the Draft Data Protection Law has not been adopted to date. Nevertheless, it is expected that the Draft Data Protection Law is adopted in its current text within the following year.

The Draft Data Protection Law represents a copy of the GDPR in its biggest part. Nevertheless, it should also be noted that it does not envisage any of the recitals introduced by the GDPR and, thus, lacks the explanations as a very important tool for its full understanding and adequate application.

The overview of the most important rules governed by the Current Data Protection Law, compared with the relevant GDPR rules, follows in Section 2 of this Chapter II. The relevant secondary legislation will also be covered by the respective overview. Section 2 also provides a brief overview of the rules foreseen by the Draft Data Protection Law.

The authority competent for data protection matters in Bosnia and Herzegovina is the BiH Data Protection Agency ("**Agency**"). The Agency is seated in Sarajevo and its official website is www.azlp.ba.

The Agency was established by the Current Data Protection Law as the authority with the exclusive competence in the field of protection of personal data. There was no such authority in BiH prior to its establishment. The main challenges which the Agency regularly emphasises in its reports are the insufficiency of staff, particularly in the field of inspection supervision and lack of financial means within the allocated budget. Further information on the Agency is provided in Section 3 of this Chapter II.

2. ASSESSMENT OF THE LEVEL OF COMPLIANCE OF THE DATA PROTECTION LAW AND RELEVANT SECONDARY LEGISLATION WITH GDPR

As noted above, the Current Data Protection Law is not aligned with the GDPR.

This overview contains summary of the most important rules and areas governed by the Current Data Protection Law, as well as the identification of the most important secondary legislation and matters prescribed by such legislation, as follows: (1) general data processing requirements, (2) obligations and responsibilities of data controllers and data processors, (3) representatives of foreign entities, (4) special categories of personal data, (5) rights of data subjects, (6) registration and records of data processing activities, (7) data transfer, (8) penal policy, and (9) relevant secondary legislation.

As noted above, at the end of each point below, we have also given a short overview of the respective topic as per the Draft Data Protection Law.

1. GENERAL DATA PROCESSING REQUIREMENTS

Under the Current Data Protection Law, all personal data, regardless of their type, category of data subjects and scope of particular processing, should be processed in line with certain processing principles explicitly governed by the respective law, as follows: (1) personal data should be processed for specified, explicit and legitimate purposes, (2) processing should be carried out lawfully and fairly, (3) processing should be limited to data which is necessary for fulfilment of the processing's purpose(s), (4) processed data should be accurate and, where necessary, kept up to date, and incorrect and incomplete data must be deleted or corrected, (5) processed data should not be retained longer than necessary for the purpose(s) for which they are processed, and (6) personal data obtained for various purposes may not be combined or merged.

The above-mentioned requirement of carrying out the data processing lawfully means that, amongst other, it should be based on adequate legal grounds. Such legal grounds is either a data subject's consent (relating to specified, explicit and legitimate purpose(s)) or one of the remaining grounds explicitly prescribed by the Current Data Protection Law. Specifically, these grounds include: (1) necessity for compliance with a legal obligation to which the data controller is subject, (2) necessity of a particular processing for the performance of a contract to which a data subject is party or in order to take steps at the request of the data subject prior to entering into a contract, (3) necessity for the protection of the vital interests of the data subject (in which case the consent must be obtained without delay or the processing has to be terminated and collected data destroyed), (4) necessity for the performance of a task carried out in the public interest, (5) necessity for fulfilment 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, and (6) necessity for implementation of legitimate activities of political parties, movements, civic associations, trade union organisations and religious communities, except where such interests are overridden by the

interests or fundamental rights and freedoms of the data subject which require protection of personal data ("**Statutory Grounds**").

It is evident that each of the Statutory Grounds includes necessity of a particular data processing to achieve a specific legitimate purpose(s).

The legal grounds (i.e. a data subject's consent and the Statutory Grounds) envisaged by the Current Data Protection Law do not fully correspond to the data processing legal grounds envisaged by the GDPR. Specifically, in case of processing for the purpose of protection of the vital interests of the data subject, the Current Data Protection Law, unlike the GDPR, foresees the obligation of the controller to obtain the data subject's consent without delay or to terminate the processing and destroy the collected data. Further, one of the Statutory Grounds foreseen by the Current Data Protection Law is the necessity for implementation of legitimate activities of political parties, movements, civic associations, trade union organisations and religious communities, which is not recognised as legal grounds for the general data processing by the GDPR.

When it comes to the above-identified data processing requirements, they are generally aligned with the relevant GDPR requirements, but certain differences exist. For example, the Current Data Protection Law does not envisage, at least not explicitly, the GDPR principle which foresees that processing must be performed in a manner that the appropriate processed data security in ensured.

On the other hand, the legal grounds (i.e. a data subject's consent and the Statutory Grounds), as well as the data processing requirements envisaged by the Draft Data Protection Law fully correspond to those envisaged by the GDPR.

2. OBLIGATIONS AND RESPONSIBILITY OF DATA CONTROLLERS AND DATA PROCESSORS

Data controllers and data processors are obliged to perform data processing in compliance with all the data processing principles described above.

The respective objective should be achieved by implementing appropriate technical, organisational and human resources measures, whereas the nature, scope, context and purposes of the particular processing, as well as the risks of varying likelihood and severity to the rights and freedoms of natural persons, should be taken into consideration. The measures should ensure adequate protection of the processed data including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. The rights of data subjects should be duly protected.

Further, a data controller, and, within the scope of its competencies, a data processor, are required to develop a data security plan, which specifies technical and organisational measures for data security, as well as the instruments for implementation of the respective measures. The same as the GDPR, the Current Data Protection Law does not prescribe the exhaustive list of the respective measures, but solely provides some examples (such as, for example, password protection and similar) and describes, in general, their purpose and circumstances to be taken into consideration when deciding on their implementation.

When it comes to the relationship between a data controller and a data processor, a written data processing agreement should be entered into between them. The mandatory provisions of the data processing agreement include the scope, purpose and duration of the processing. Further, a data controller should only engage a data processor which provides sufficient guarantees that the appropriate technical and organisational measures shall be undertaken to provide data security. It is also prescribed that a data processor may process the data only on the data controller's instructions and may not engage another processor (i.e. sub-processor) without prior written authorisation of the data controller.

3. REPRESENTATIVES OF FOREIGN ENTITIES

Under the Current Data Protection Law, if a data controller which does not have the registered seat on the territory of Bosnia and Herzegovina uses automatic or other equipment located on the BiH territory for data processing, it is obliged to appoint its representative for such processing, unless the respective equipment is used solely for the transit of data through BiH.

Considering the above, it can be concluded that, when it comes to representatives of foreign entities, the concept of the Current Data Protection Law is completely different from the concept of the respective representative appointment under the GDPR (for example, one of the cases when such appointment is obligatory under the GDPR is the case when a non-EU entity offers services to natural persons in the EU, whereas it is irrelevant whether any equipment which such entity uses for the respective data processing is located in the EU).

It should also be noted that, again differently in comparison to the GDPR, the respective representative appointment obligation is prescribed solely for foreign data controllers (i.e. foreign data processors remain out of its scope).

On the other hand, the rules envisaged by the Draft Data Protection Law with regard to the representatives of foreign entities performing the relevant data processing activities are aligned with the GDPR.

4. SPECIAL CATEGORIES OF PERSONAL DATA

The definition of special categories of personal data, as prescribed by the Current Data Protection Law, is not fully aligned with the respective GDPR definition. Specifically, special categories of personal data under the Current Data Protection Law, include data revealing racial, national or ethnic origin, political opinion or political party's affiliation, religious or philosophical or other beliefs, trade union membership, genetic code, biometric data, health condition related data, data concerning a natural person's sex life and personal data related to criminal convictions. Accordingly, when we compare this definition with the GDPR definition of special categories of personal data, it can be concluded that some "elements" of the GDPR definition are missing (such as the data concerning a natural person's sex orientation), while some other are envisaged by the Current Data Protection Law although they are not considered as special categories of personal data by the GDPR (such as the data related to criminal convictions).

The Current Data Protection Law also prescribes that any processing of special categories of data is generally prohibited. However, this is not an absolute prohibition, i.e. their processing is allowed in certain exceptional cases explicitly prescribed by the Current Data Protection Law: if a data subject has given explicit consent to the processing of such data, or if their processing is necessary for the purposes of carrying out the obligations/exercising specific rights of the data controller in the field of employment, or processing relates to personal data which are clearly made public by the data subject, or processing is necessary for the establishment, exercise or defence of legal claims, or if the processing is carried out to serve the needs of preventive medicine, medicinal diagnostics, medical service providing and management, provided that such data are processed by a professional medical officer (or other person) who is obliged to keep the professional secret, or if the processing is of particular public interest, or if the data processing is carried out within the scope of legitimate activities of an institution, foundation, association or any other non-profit organisation with political, philosophical, religious or trade union objectives, provided that the data processing shall solely relate to the members of the bodies or persons who have regular contacts with them in reference to their objectives, and the data shall not be disclosed to a third party without the consent of the data subject and other cases prescribed by the Current Data Protection Law ("**Exceptional Cases**").

When we compare the Exceptional Cases under the Current Data Protection Law and under the GDPR, it can be concluded that the respective lists are quite similar, but not the same, plus the GDPR envisages some cases which are not recognised by the Current Data Protection Law, for example if processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

The definition and further rules on processing of special categories of personal data, as prescribed by the Draft Data Protection Law, correspond to the respective GDPR rules.

5. RIGHTS OF DATA SUBJECTS

The Current Data Protection Law envisages a set of rights which belong to data subjects in relation to their personal data processing. Exercise of these rights may be conditioned on fulfilment of certain requirements and/or may be limited depending on the circumstances of each particular case. The Law explicitly governs such requirements/limitations as well ("**Prescribed Restrictions**").

In general, the following rights are subject to the Prescribed Restrictions : (1) right to request information on a particular processing, (2) right to access the processed data and to obtain their copy, (3) right to rectification, (4) right to deletion, (5) right to restriction of the data processing (e.g. if the processed data's accuracy is contested by the data subject), (6) right to object to the data processing (e.g. if the processing is based on the legitimate interest or performed for direct marketing purposes) and to the processing's cessation, (7) right to withdraw consent (where consent is a legal ground for processing), and (8) right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning the data subject or significantly affects him/her ("**Relevant Rights**").

As opposed to the GDPR, the Current Data Protection Law does not explicitly prescribe the procedure or deadlines within which the controllers are obliged to ensure exercise of the Relevant Rights, the exception being the right to access and to obtain the copy of data which must be exercised within a 30 day-term. If a data subject finds or suspects that the controller or processor breached the data subject's right, or that there is a direct risk of breach of right, the data subject may file a complaint with the Agency for the purposes of protecting his/her rights ("**Data Processing Complaint**") and thereby request (i) that the controller or processor refrains from such activities and remedies the factual situation caused by such activities, or (ii) that the controller or processor carries out a correction or amendment of personal data so as to make them authentic and accurate, or (iii) that the personal data is blocked or destroyed.

Also, any person who considers that any of his/her rights was infringed by processing activities of a data controller/processor is entitled to the court protection of his/her rights.

Although the Current Data Protection Law provides all rights foreseen by the GDPR, except the right to data portability, the manner of exercising these rights is regulated poorly under the Current Data Protection Law, i.e. in many points it lacks details on the manner of exercising these rights or the deadline within which the data controller/processor is obliged to ensure the exercise of the Relevant Rights.

On the other hand, the rights of data subjects and the manner of exercising these rights foreseen by the Draft Data Protection Law are aligned with the GDPR.

6. REGISTRATION AND RECORDS OF DATA PROCESSING ACTIVITIES

The Current Data Protection Law obliges data controllers to keep (manually or by means of automatic data processing tools) records (of prescribed content) for each database containing personal data which they establish. They are also obliged to register their databases with the Agency, i.e. to provide the Agency with certain information on each of the respective databases which consolidates the provided data into the so-called Central Registry.

Additionally, if their databases are maintained automatically, in full or partially, they are obliged, subject to certain exceptions, to submit to the Agency a request regarding the intended establishment of each of the respective databases, prior to undertaking any data processing activities. If the involved automatic processing bears a risk for the data subject's rights, the data processing activities may commence only after the Agency approves the processing or upon expiry of two months following the day when the Agency received the request.

Based on the above, it can be concluded that both the Current Data Protection Law and the GDPR establish the obligation of keeping records of data processing activities (keeping, however, in mind that, under the GDPR, such obligation is applicable to both data controllers and data processors and only in certain cases, i.e. only for certain types of the respective entities and/or data processing activities). On the other hand, the database registration obligation is not envisaged by the GDPR at all, and, from that point of view, the Current Data Protection Law is not aligned with the GDPR.

On the other hand, the Draft Data Protection Law foresees the obligation of data controllers and data processors to keep records of their data processing activities identically as the GDPR, i.e. it does not oblige data controllers to register their data processing activities/ databases with the Agency.

7. DATA TRANSFER

As per the Current Data Protection Law, personal data may be transferred to another economy or an international organisation that implements adequate safeguards for personal data set by the Current Data Protection Law. Adequacy of safeguards is evaluated on the basis of specific characteristics of each particular transfer, such as the types of personal data, purpose and period of the processing, economy to which data is to be transferred, statutory rules in force in the respective economy and other relevant circumstances.

Further, personal data may also be transferred to an economy which does not provide adequate safeguards in the aforementioned sense in the following cases envisaged by the Current Data Protection Law: the disclosure of personal data is provided by special law or international treaty binding for BiH; prior consent was obtained from the person whose data are transferred and the person was informed on the potential consequences of the data transfer; the disclosure of personal data is necessary for fulfilling the contract between the data subject and the controller or the fulfilment of pre-contractual obligations undertaken at the request of the person whose data are processed; the disclosure of personal data is necessary to save the life of the person to whom the data pertains or when it is in his/ her vital interests; the personal data are transferred from the files or records which are, in accordance with the law or other regulations, available to the public; the transfer of personal data is necessary for the reasons of public interest; the transfer of personal data is necessary for concluding or fulfilling a contract between the controller and a third party when the contract is in the interest of the data subject.

Exceptionally, even if none of the aforementioned cases is applicable, the data can be legitimately transferred out of Bosnia and Herzegovina if the Agency approves such transfer and if a data controller in that economy provides adequate safeguards for the protection of privacy and fundamental rights and freedoms of individuals or provision of similar rights arises from the provisions of a special agreement.

The Draft Data Protection Law prescribes a set of mechanisms based on which a legitimate transfer of data out of BiH is possible. This means that the Draft Data Protection Law tends,

the same as the GDPR, to enable legitimate transfer of personal data whenever there are some safeguards that transferred data will be processed in line with the law.

Specifically, in brief, this means the following:

1. It should firstly be checked whether a particular economy to which the data is to be transferred is regarded as an economy with an adequate data protection system ("**Adequate Economy**")
2. If an economy to which the data is to be transferred from BiH is the Adequate Economy or if there is a data transfer related international treaty entered into between BiH and that economy, a transfer is possible without any approval of the Agency ("**Transfer Approval**");
3. On the other hand, if an economy to which the data is to be transferred is not the Adequate Economy, a transfer is still possible without the Transfer Approval if the adequate data protection measures are undertaken (e.g. if appropriate standard contractual clauses have been entered into between a data exporter and a data importer) ("**Adequate Safeguards**");
4. However, even if there are no Adequate Safeguards, there is still a possibility for transferring the data without the Transfer Approval. Such possibility exists in so-called special situations, explicitly stipulated by the Draft Data Protection Law, the same as under the GDPR (e.g. a data subject has consented to a particular transfer, a transfer is necessary for the performance of an agreement between a data subject and data controller, etc.);
5. Finally, even if none of the aforementioned special situations is applicable, a data transfer is still allowed without the Transfer Approval if certain conditions (linked to a data controller's legitimate interest) explicitly stipulated by the Draft Data Protection Law are cumulatively fulfilled.

8. PENAL POLICY

If we would have to identify the most significant difference between the Current Data Protection Law and the GDPR, the penal policy would certainly be the one.

This is due to the fact that, unlike very stringent penal policy and extremely high fines introduced by the GDPR (i.e. fines in the amount of up to EUR 20,000,000 or 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher), the Current Data Protection Law has a very mild penal policy.

Specifically, it prescribes offence liability for breaching the law, whereas the highest amount of the fine for such breaches is BAM 100,000 (approx. up to EUR 50,000) for a legal entity and BAM 15,000 (approx. up to EUR 7,000) for a legal entity's representative or a natural person, per offence.

On the other hand, the Draft Data Protection Law, although still not as strict as the GDPR, foresees fines which are significantly higher than the ones foreseen by the Current Data Protection Law. Specifically, the Draft Data Protection Law introduces fines in the amount of up to BAM 200,000 (approx. EUR 100,000) or 4% of the total worldwide annual turnover of the preceding financial year (whichever is higher).

9. RELEVANT SECONDARY LEGISLATION

In addition to the Current Data Protection Law, a following set of subordinate legislation (i.e. rulebooks) was adopted in 2009:

1. The Rulebook on the Manner of Keeping Records of Databases and Pertinent Records Form;
2. The Rulebook on the Manner of Keeping and Special Measures of Personal Data Technical Protection;
3. The Rulebook on the Procedure following the Complaint of the Data Subject to the Data Protection Agency of Bosnia and Herzegovina; and
4. The Rulebook on Supervision Inspection Regarding Personal Data Protection.

This legislation governs the following issues introduced by the Current Data Protection Law:

I. **Records of Data Processing Activities** – as mentioned above under point 6, data controllers are generally obliged to establish the records for each of their databases containing personal data and register the respective data processing activities with the Agency (i.e. in the so-called Central Registry).

   The Rulebook on the Manner of Keeping Records of Databases and Pertinent Records Form governs the respective issues, as well as the applicable exceptions and forms, in detail.

   Specifically, the Rulebook on the Manner of Keeping Records of Databases and Pertinent Records Form stipulates that records of databases must include the following:

   1. Name of the record - to be determined by the controller by the adoption of the decision which shall regulate the name of the record, as well as the manner and purpose of data processing, in case there is no legal provision prescribing determination of the name;
   2. Name and address of data controller and data processor;
   3. Purpose of data processing - shall contain the description of the purpose of collecting the personal data and shall indicate whether the purpose is established by law or by the personal data filing system controller upon the data subject's consent;
   4. Legal basis for data processing – shall contain the exact provision which serves as legal basis for data processing or the information regarding the data subject's consent in case data processing is performed based on a consent;
   5. Type of data that is being processed and categories of data subjects;
   6. Origin and manner of collecting the personal data - the data about the origin of personal data shall be given in the records by indicating the source of information (directly from the data subject; from other data filing systems kept by the same data controller; from a third party whose name shall be given; by import from another data controller whose name shall be given; by personal observation, research or from other sources that shall be specified in the records). The manner of collecting the information shall refer to the data medium from which the information is obtained (e.g. cassette, floppy disk, web, information given verbally or in writing, medical check-up or any other manner of obtaining the personal data that is specified in detail in the records);
   7. Types of transferred data, users and legal grounds - shall contain the list of all types of personal data accessible to users, with user's references and the title of the law governing the access to such personal data;
   8. Deadline for deletion of processed data – if the period of use of personal data is not stipulated by a special act, the records shall contain the period necessary for the fulfilment of the purpose for which the personal data were collected;
   9. Information about the measures undertaken for data protection;
   10. Information on transfer of data abroad - in the event of import or export of personal data to and from Bosnia and Herzegovina, the records of the personal data filing

system shall indicate the name of the economy or international organisation and foreign user of personal data, as well as the purpose of import or export stipulated by an international agreement, act or any other regulation, or by the data subject's written consent.

Each record, as well as any amendment thereto shall be assigned a numerical code determined by the controller in accordance with the time of origin and establishment of the databases record. If the name of the database record is not determined by a special law, the name is determined by the data controller by way of a special decision setting forth the manner and purpose of the personal data processing. The content thereof must match the group of personal data contained in the database concerned or the category of the data subjects. The name and seat of the data controller shall comply with the registered name and the seat of the legal or natural person or legally established name for the government authority.

As mentioned above under point 6, it can be concluded that both GDPR and the Current Data Protection Law establish the obligation of keeping records of data processing activities, however, while the database registration is not envisaged by the GDPR, pursuant to the Rulebook on the Manner of Keeping Records of Databases and Pertinent Records Form, data controllers are obliged to register data processing activities with the Agency in the so- called Central Registry.

In the light of aforementioned, the Rulebook on the Manner of Keeping Records of Databases and Pertinent Records Form is not aligned with the GDPR.

II. **Technical and organisational measures undertaken to provide data security** – data controllers are obliged to draft a data safety plan for the sake of ensuring confidentiality, integrity, availability, authenticity, possibility of revision, and transparency of data processing.

The Rulebook on the Manner of Keeping and Special Measures of Personal Data Technical Protection stipulates this obligation, as well as general measures for personal data keeping and personal data protection.

Pursuant to the Rulebook on the Manner of Keeping and Special Measures of Personal Data Technical Protection, the data safety plan must include technical and organisational measures that shall ensure that:

1. Data is known only to authorised persons - confidentiality;
2. Data remain unchanged, complete and up to date during processing - integrity;
3. Data is constantly available and can be processed correctly - availability;
4. The origin of data can be established at any time - authenticity;
5. It can be determined who, when, what data was processed and in what way - possibility of audit;
6. The procedure for processing data is complete, up to date and duly recorded - transparency.

During the automatic processing of data, the controller should ensure technical measures as follows:

1. Unique username and password composed of a combination of at least six characters, numbers or letters;
2. Automatic password's change after a specified period of time, which may not exceed six months;
3. Username and password will allow access only to the parts of the system required for execution of work tasks;

4. Automatic logout from the system after the expiration of a certain period of inactivity, not longer than 15 minutes, re-entering username and password is necessary for reactivating the system;
5. Automatic denial of access to the system after three unsuccessful attempts to log in to the system and automatic warning to seek instructions from the data collection administrator;
6. Effective and secure antivirus protection of the system, which must constantly be updated to prevent the unknown or unplanned dangers of new viruses;
7. Computer, software and other necessary equipment must be connected to the electricity network via a device for uninterruptible power supply.

Further, the controller in the automatic data processing should also ensure organisational measures for the protection of data, as follows:

1. Complete secrecy and security of passwords and other forms of identification of access to data;
2. Organisational rules for the provider's access to the Internet relating to the downloading and recording of documents via e-mail or other sources;
3. Destruction of documents containing personal data after the processing deadline;
4. Any display of any media containing personal data outside the work premises must be with a special permission and control to prevent loss or illegal use;
5. Measures for the physical protection of work premises and equipment where personal data are processed; and
6. Compliance with technical instructions when installing and using equipment used for personal data processing.

When processing special categories of personal data, the controller must indicate that special categories of data are being processed, and ensure the following:

1. Ability to identify each individual authorised access to the information system;
2. Work with data during the regular working hours; and
3. Crypto protection of data during transmission over telecommunication systems with appropriate software and technical measures.

Even though GDPR envisages that the controller should use appropriate procedures and technical, as well as organisational measures while processing data in order to ensure fair and transparent processing, GDPR does not impose an obligation of drafting a data safety plan, hence it can be concluded that the Rulebook on the Manner of Keeping and Special Measures of Personal Data Technical Protection is not aligned with the GDPR.

III. **Communication with the Agency in case of complaint** - the Data Processing Complaint, as defined under point 5 herein, should be filed with the Agency in the procedure prescribed by the Rulebook on the Procedure following the Complaint of the Data Subject to the Data Protection Agency of Bosnia and Herzegovina.

The Data Processing Complaint should, as a minimum contain (i) name, surname and address of the complainant or a note that the complainant wishes to remain anonymous; (ii) name of the data controller or processor against whom the complaint is filed; (iii) a brief explanation of the complaint; (iv) evidence supporting the complaint; and (v) handwritten signature of the complainant or the proxy in which case the power of attorney shall be attached to the complaint. In line with the Law on Administrative Procedures, the deadline for resolving the Data Processing Complaint is 30 or 60 days depending on the complexity of the matter.

Prior to reaching the decision regarding the Data Processing Complaint, the Agency is obliged to determine all facts and circumstances important for decision-making and to enable the data controller or processor to exercise and protect their rights and legal interests. The facts and circumstances relevant for resolving the Data Processing Complaint may be established in a simplified or in a special inquiry procedure. The Agency shall make it possible for the complainant and the data controller or data processor to give written statement on all facts and circumstances as well as on all proposals and offered evidence. The Agency may undertake official activities during the procedure in order to establish the factual situation.

The Agency may decide on a Data Processing Complaint under the simplified procedure in the following cases:

1. If the complainant has stated facts and submitted evidence based on which the situation can be adequately assessed or if the situation can be determined based on generally known facts or facts known to the Agency;
2. If the matter may be assessed based on the official data held by the Agency, and it is not necessary to hold a hearing with the complainant, the data controller or processor in order to protect their rights or legal interests;
3. In the case it is necessary to undertake emergency measures of public interest that cannot be postponed, and the facts on which the decision is to be based have been determined or at least made probable.

The special investigation procedure is conducted when necessary in order to establish facts and circumstances important for clarification of the matter and enabling the complainant and the data controller or processor to exercise and protect their rights and legal interests. The course of the investigation procedure is determined according to circumstances of a specific case, including but not limited to: determining which procedural acts are to be executed and issuing orders for their execution, determining on the sequence of actions and deadlines of their execution, deciding on which evidence are to be drawn and by which means, as well as deciding on all proposals and statements.

The facts based on which the decision on the Data Processing Complaint is made are established through evidence. The Agency officials decide if a fact is to be proved or not, depending on whether the fact may influence the resolution of the matter. If the Data Processing Complaint cannot be resolved based on the described factual status and provided evidence, the Agency shall perform inspection in order to determine the relevant facts.

The Agency shall reject the Data Processing Complaint as unfounded if it determines that the data controller or processor processed the personal data in line with the basic data processing principles and the rights of the data subject were not violated, and especially if it determines that:

1. The undertaken actions do not represent data processing;
2. The processing is made by the natural person for own purpose only;
3. The processing is performed in accordance with the applicable regulations;
4. The processing is performed with the data subject's consent, and such consent is not suspicious; and
5. The processing was conducted without the data subject's consent, in cases prescribed by the law.

The Agency shall issue the decision accepting the Data Processing Complaint if it determines that the data controller or processor conducted the processing contrary to the basic data processing principles and violated the rights of the data subject. In case the Agency accepts the Data Processing Complaint, it may order to the data controller or processor the following measures: (1) personal data blocking; (2) personal data erasing or destroying; (3) personal data correction or amendment; (4) temporary or permanent ban on data processing; and (5) warning.

No appeal can be filed against a decision passed by the Agency, but an administrative dispute can be initiated against such decision before the BiH Court.

As mentioned above under point 5, in case a data subject finds or suspects that the controller or processor breached the data subject's right, or that there is a direct risk of breach of right, the data subject may file a complaint with the Agency. The rights of the data subjects and the manner of exercising these rights foreseen by the Draft Data Protection Law are aligned with the GDPR, while the Current Data Protection Law lacks details on the manner of exercising of the rights, unlike the GDPR.

IV. **Supervision by the Agency** – conducting supervision inspection by the Agency in order to ensure application of the Current Data Protection Law, and other regulations on processing of personal data, jurisdiction, responsibility and manner of conducting of supervision inspection, rights and duties of inspectors, minutes on supervision inspection and manner of imposing administrative measures, records on completed supervision inspection, as well as other issues related to supervision inspection are regulated by the Rulebook on Supervision Inspection Regarding Personal Data Protection.

Pursuant to the Rulebook on Supervision Inspection Regarding Personal Data Protection, the inspection supervision can be initiated by the inspectors on the basis of the approved inspection work plan, upon filed complaint of the data subjects, and upon the order of the Director of the Agency in case of suspicion that the provision of Current Data Protection Law may be breached.

The supervision inspection makes a direct insight into the legality of work of the data controllers and data processors, and implementation of administrative measures for prevention and elimination of illegal application of regulations in the area of personal data protection. The supervision inspection also has a preventive purpose to induce discipline in application of regulations in the area of personal data protection.

Supervision activities are conducted by the inspectors. The inspectors have the right and duty to perform direct check of business premises and other facilities for processing of personal data, the work process, personal and other documents. They also perform other activities in line with the purpose of supervision inspection. All data controllers and processors are obliged to enable the inspectors to supervise and look into the required data and materials, to supply necessary information and data of importance for the supervision. The inspectors are obliged to keep confidential all data obtained during the inspection.

While conducting the supervision inspection, the inspectors have the right to directly perform the following:

1. To enter all premises for processing of personal data. Entrance and control of assets and the room of the data controller or processor, which are not provided by the law, may be carried out only during the working hours;
2. To request from the data controller or processor to submit for review any document or records containing personal data, and supply any information on any issue whatsoever upon request;
3. To request from the data controller or processor to terminate illegal processing of personal data, and order other measures which the data controller or processor is

obliged to undertake without delay and notify the Agency thereon in written form within 15 days.

The supervision inspection is generally conducted in compliance with the Agency's annual and monthly inspection programmes of work. The annual inspection programme includes the survey of all areas to be encompassed by regular supervision inspection in a specific calendar year. The proposal of the annual inspection programme for the following year is made by the Assistant Director in the Sector for Supervision Inspection, Complaints and Main Registry no later than the end of November of the current year, and it is approved by the Agency Director. The monthly programme of work includes survey of individual inspections with exact data on controllers. The monthly inspection programme for the following month is made by the Head of the Division for Supervision Inspection and Complaints no later than the 10th day of the current month for the following month, and it is approved by the Assistant Director in the Sector for Supervision Inspection, Complaints and Main Registry. Upon complaint filed by the data subject, the Agency undertakes appropriate measures and activities in order to establish the soundness of the complaint. The supervision inspection shall also be conducted if the case, upon the complaint, cannot be resolved based on existing facts and evidence.

Usually a written notice to the controller or processor is served 5 days before the day of inspection supervision, and it contains information regarding the purpose of the inspection, time, place and tasks to be performed by the inspectors. However, the aforementioned written notice shall not be delivered to the controller or processor if it would jeopardise the purpose of inspection.

The order for supervision inspection is issued in writing and it contains:

1. The name of the person who issued the order, number and date;
2. The name of the data controller or processor, seat and address where the supervision inspection shall take place;
3. The purpose of supervision inspection;
4. The subject of supervision inspection;
5. Legal grounds for conducting the supervision inspection;
6. Name and surname of the inspector who will conduct supervision inspection;
7. Starting date of the supervision inspection;
8. Signature of the order issuer.

The inspection supervision is performed by:

1. Undertaking inspection activities to determine the situation in the field of data processing and protection;
2. Determining administrative measures for the purpose of preventing and eliminating illegalities in the implementation of regulations in the field of data processing and protection;
3. Undertaking other measures and actions determined by the Current Data Protection Law, and relevant secondary legislation.

If, during the inspection, the inspector determines violations of the applicable legislation, he/she has a right and is obliged to order the following measures:

1. To eliminate the identified deficiencies and irregularities within 15 days;
2. To block, delete or destroy personal data, temporarily or permanently prohibit processing, to warn or issue a notice to the controller or processor;
3. To prohibit the processing of personal data that is contrary to the basic principles of lawful processing of personal data and the rights of data subjects;
4. To impose and collect a fine;
5. To take other administrative measures and actions that it deems necessary.

When the ordered measure concerns the activities that must be carried out in a specific time limit, the controller who was ordered to undertake the measure shall immediately notify the Agency in written form on the completed activity, and not later than 15 days from the receipt of the decision. The notification on execution of specific activities may be delivered verbally upon the minutes made by the inspector who conducted the supervision inspection. The inspector must officially, as his duty, follow up and confirm the execution of the administrative measure. The inspector confirms the execution of the administrative measure based on the revision inspection or other evidence and makes special minutes or an official note thereon.

The inspector may also take appropriate preventive activities in order to prevent the occurrence of harmful consequences due to deficiencies and irregularities in the implementation of the Current Data Protection Law, other laws and regulations on the basis of which the processing of personal data is executed, such as:

1. A warning to the controller or processor on the obligations from the above regulations;
2. Pointing out the harmful consequences;
3. Proposing measures to eliminate their causes;
4. Other preventive activities.

Upon the completed supervision inspection, the inspector shall make the minutes containing the determined factual situation. The minutes are a public document, except for the minutes or parts of the minutes containing confidential data. The data controller or processor which was the subject of inspection has the right to file a complaint on the minutes immediately at making of the minutes, or if the minutes are delivered subsequently (during complex supervision inspection the minutes may be made in the official premises of the Agency within 3 days from the date of completion of the supervision inspection) within 3 days from the receipt of the minutes.

In case the conducted inspection supervision results in an adoption of a decision, the controller or processor is entitled to submit an appeal to the Agency on the issued decision within 8 days from the receipt of the decision. The decision upon submitted appeal needs to be rendered within 15 days from the submission. An administrative dispute may be also initiated before the BiH Court against the appeal decision.

In the light of everything aforementioned, it can be concluded that the supervision of the implementation of the Current Data Protection Law stipulated by the Rulebook on Supervision Inspection Regarding Personal Data Protection is partially aligned with the GDPR.

3. COMPETENCE OF AND CHALLENGES IN THE WORK OF THE AGENCY

The public authority with the competence in the field of data protection is the Personal Data Protection Agency (in Bosnian, *Agencija za zaštitu ličnih podataka*).

Under the Current Data Protection Law, the Agency is an autonomous administrative organisation established for the purpose of ensuring the protection of personal data.

The Agency is headed by the director, who is liable for the work of the Agency to the BiH Parliament.

Nevertheless, considering that the Agency is a public authority, financial resources for its work are provided in the government budget in line with the law on budget and laws governing public administration and position of public servants. Information on the exact purposes for which the budget resources provided to the Agency are spent (e.g. salaries of employees, travel expenses, expenses for office equipment and materials, etc.) and on the exact amount of each of such spending are published in the report on budget expenditure for the respective year, which is available on the Agency's website.

The Agency is also obliged to prepare an annual report on its activities and to submit such report to the BiH Parliament.

The Agency's competences are set in detail by the Current Data Protection Law (e.g. monitoring the respective law implementation, acting upon complaints of data subjects, adopting secondary regulations, guidelines or other legal documents, etc.). The Draft Data Protection Law foresees that as of the day of its entry into force, the Agency will be renamed to the Data Protection Commissioner.

For the purpose of exercising its authorisations and duties within its sphere of competence, the Agency basically has two types of powers:

1. Powers relating to its capacity of a second-instance authority responsible for protecting the right to data protection in complaint proceedings (i.e. based on the Data Processing Complaints filed with the Agency) ("**Complaint Related Powers**"), and
2. Powers relating to its capacity of a supervisory authority responsible for enforcing the Current Data Protection Law ("**Supervisory Powers**").

When it comes to the Agency's Complaint Related Powers, as noted above under Section 2 of Chapter II of the report, it decides on filed complaints within 30 or 60 days (depending on the complexity of the complaint) from the day of their filing, whereas it firstly forwards the complaints to the data controller or processor responsible for undertaking data processing activities which the complaints were filed against for their comments. Depending on whether the Agency finds a complaint grounded, it may reject it (if ungrounded) or order the data controller or processor to act upon the request within a specified period of time (if grounded). In any case, no appeal can be filed against a decision passed by the Agency, but an administrative dispute can be initiated against such decision before the BiH Court.

When it comes to the Agency's Supervisory Powers, the Agency (through its inspectors) is entitled, amongst other, to issue resolutions ordering certain corrective measures to data controllers/processors (e.g. to order them to rectify the determined deficiencies with a 15-day period, stop undertaking particular data processing activities, etc.), as well as to issue fines. The controller/processor may file an appeal against the resolution to the Director of the Agency. An administrative dispute can be initiated against the second instance resolution of the Director with the BiH Court.

The support (other than the aforementioned government budget allocation) the Agency (potentially) receives for the purpose of further development of data protection policies and practice in Bosnia and Herzegovina is important for its work and organisation. Based on the information publicly available (contained in the yearly reports published by the Agency), the Agency did not participate in a significant number of projects which were not funded through the budget. However, we did identify the following projects:

1. **Support to the Agency for Personal Data Protection in BA** project implemented in 2009 and financed by the European Commission aimed at strengthening the capacities of the Agency upon its establishment;
2. **TAIEX (Technical Assistance and Information Exchange instrument of the European Commission) expert mission** conducted with the aim to discuss important steps in drafting a new Law on Personal Data Protection organised in October 2017;
3. **Project of translation of the Draft Data Protection Law** to English for the purpose of its review by experts from Great Britain, financed through IPA 2017.

There are no projects published on the Agency's website as its current projects. It should nevertheless be mentioned, for the sake of completeness, that, when it comes to cooperation between the data protection authorities in the region, the Initiative 2017 was established. This group is consisted of data protection authorities from the following seven jurisdictions in the region: Bosnia and Herzegovina, Serbia, Montenegro, Republic of North Macedonia, Croatia, Slovenia and Kosovo*. So far, 3 meetings of the group were held. The last one was held from 26 to 28 May 2019 in Montenegro and focused on then current state of alignment of the respective jurisdictions' legislation with the GDPR. It remains to be seen how much/whether this group (and the Agency as its part) shall be active in the future, considering particularly the fact that, as already mentioned at the beginning of this report, the GDPR aligned data protection law still remains to be adopted and implemented in Bosnia and Herzegovina. In any case, more information on this group is provided in Chapter II, Section 5 herein.

In addition to the Agency, there are several other government authorities with competence in the field of data protection. Below is a brief summary of their position and data protection related competences.

BiH Parliament represents an institution of major importance in the field of data protection, given that it is the highest-level legislative body of Bosnia and Herzegovina, and has other important supervisory competences in the field of data protection, as elaborated in detail below.

The BiH Parliament is established by the BiH Constitution and consists of two Houses: (i) the House of Representatives, and (ii) the House of Peoples, and all legislative decisions enter into force upon adoption by both Houses of the BiH Parliament. The House of Representatives comprises 42 members elected by vote on the basis of proportional representation and has 7 standing committees. The House of Peoples has 15 delegates, designated by the Federation of Bosnia and Herzegovina's House of Peoples and the Republika Srpska's National Assembly, and has 3 standing committees.

A proposed draft law may be introduced by any representative, or a delegate, committee of the House, joint committee of both Houses, the House of Representatives, the House of Peoples, as well as the BiH Presidency and the BiH Council of Ministers within the scope of their respective competencies. Afterwards, the Collegium of each House submits the proposed draft law to the appropriate Constitutional and Legal Committee and a committee responsible for providing the opinion about the proposed law. The Constitutional and Legal Committee considers, in the first stage, whether the proposed draft law is harmonised with the BiH Constitution and the legal system, while the responsible committee discusses its principles.

In case both committees provide positive opinions, the discussion on constitutional grounds and principles which the proposed law is based on is initiated, and adoption of the proposed law is in accordance with the opinions by the Constitutional and Legal Committee and a responsible committee. Afterwards, the proposed law can be either adopted or rejected.

The responsible committee initiates debate on the proposed law and submitted amendments. Both Houses debate on positive report of the responsible committee and vote on the proposed amendments, following the articles related to amendments.

The next step is voting on the proposed law in its final text. A negative opinion of the responsible committee can be accepted and the proposed law rejected, or negative opinion

can be rejected and the proposed law returned to the committee for reconsideration. The adopted text of the law is harmonised with the text from the other House. If both texts are identical, the text of the law is published in the Official Gazette of Bosnia and Herzegovina thus, the legislative procedure of passing the law is completed. If the texts of the law are not identical, they need to be harmonised, and afterwards published in the Official Gazette of BiH.

Given its competences, BiH Parliament further plays an important role in approving the budget and making decisions on the sources and the amount of revenue needed for financing the institutions of BiH, including financing of the Agency.

Furthermore, the director and the deputy directors of the Agency are appointed/suspended/dismissed by BiH Parliament, and the Director of the Agency reports on his/her work directly to the BiH Parliament.

Specifically, pursuant to the Current Data Protection Law, the BiH Parliament has an authorisation to temporarily suspend the director and deputy directors in case of doubt of unlawful actions. The suspension lasts until the illegal work of the Agency is determined by a final decision.

The BiH Parliament is authorised to dismiss the appointed director and deputy directors before the end of their terms in the office in the following cases:

1. Upon their request;
2. In case of permanent inability to perform the duty;
3. In case of unlawful actions;
4. In case of the final decision determining their disciplinary responsibility;
5. In case of the imprisonment for a period exceeding six months.

BiH Council of Ministers is an executive authority body exercising its rights and carrying out its duties as governmental functions. Pursuant to the BiH Constitution, the Chairman of the Council of Ministers is nominated by BiH Presidency and confirmed by House of Representatives. The Council of Ministers is responsible for the fields of foreign policy, customs policy, monetary policy, foreign trade policy, finances of the BiH institutions, immigration, air traffic control and regulation of inter-entity transportation.

In regard to data protection, the Council of Ministers is involved in the supervision of the work performed by the Agency. More precisely, the Director of the Agency is obliged to prepare and propose for the adoption by Council of Ministers the Annual Work Plan of the Agency, as well as its annual budget, due to the procedure that requires adoption of annual budget by the Council of Ministers first and later by the BiH Parliament.

Furthermore, and as mentioned in the introduction of this report, interdisciplinary group formed by the members of the BiH Ministry of Justice, BiH Ministry of Civil Affairs, BiH Directorate for European Integration and BiH Data Protection Agency is involved in the preparation of the Draft Data Protection Law. In the light of that, BiH Ministry of Justice and BiH Ministry of Civil Affairs are also to be considered as relevant institutions in the field of data protection.

BiH Ministry of Civil Affairs is responsible, among other things, for the protection of personal data and for referring to the procedure of the current Draft Data Protection Law.

BiH Ministry of Justice is responsible, among other things, for preparation of the draft of relevant legislation, which includes legislation related to the data protection, as well as for ensuring that BiH legislation at all levels is compliant with the obligations of Bosnia and Herzegovina deriving from international agreements.

Court of Bosnia and Herzegovina is the relevant judicial authority in the field of data protection. As explained above under Chapter II, Section 3, in the field of data protection the Court of Bosnia and Herzegovina decides in an administrative dispute initiated against the decision of Agency on filed complaint as well as in a dispute initiated against the second instance decision of the Director of the Agency in regard to the decision ordering certain corrective measures to data controllers/processors with respect to the Agency's Supervisory Powers.

4. CHALLENGES IN THE IMPLEMENTATION OF THE CURRENT DATA PROTECTION LAW IN PRIVATE AND PUBLIC SECTOR

The challenges which are ahead of local entities in both private and public sector are numerous. The most difficult one is the lack of awareness on the data protection importance. For most entities (both in the public and the private sector), the obligations under the Current Data Protection Law are merely a formality, with no tendency to apply them in practice in a proper and efficient manner. The adoption of the Security Plan, as one of the most important documents that all controllers are obliged to prepare, is still unknown to the most of data processing entities, the same as it was at the beginning of the Current Data Protection Law application in 2006.

Although the Current Data Protection Law was adopted in 2006, the general public impression is that data protection is a new term and obligations stipulated by the Current Data Protection Law are merely a formality and are not to be applied in a proper manner.

However, it is encouraging that larger companies in BiH, and generally the local branches of foreign companies are starting to assess the impact of data protection on future work processes. Furthermore, legal entities in general are starting to pay more attention to data protection, mainly due to the extended territorial application of GDPR, and the high fines imposed by the latter.

Although there are certain positive developments, the percentages of legal entities that recognise the importance of data protection remains very small. The lack of awareness on importance of data protection can best be illustrated by the fact that even the entities in public sectors, and especially government authorities and agencies, are constantly committing violations of the Current Data Protection Law.

The aforementioned was clearly evident during the recent Covid-19 outbreak, which caused numerous questionable actions taken by relevant authorities while combating this global pandemic, one of them being the publication of lists containing names and addresses of the persons infected by Covid-19 and persons under mandatory self-isolation on the official websites of the relevant public authorities.

Quickly after numerous publications of these data by public authorities, the Agency emphasised that health information falls within special categories of personal data, and asserted that processing of health data under the circumstances at hand may not be justified by the public interest. In the light of this, the Agency issued a resolution prohibiting the publication of personal data of persons infected by COVID-19, as well as those subjected to self-isolation to all authorities in BiH due to the fact that such publication represents a flagrant breach of the data subject's rights guaranteed by the Current Data Protection Law[3]. The Agency confirmed[4] that it had also imposed a fine of approx. EUR 510 on 26 March 2020 to one of the authorities which published a list of people who respect house isolation on its official website – this fine was imposed to the Mayor of the City of Trebinje as this

3 Resolution of the BiH Data Protection Agency dated 24 March 2020;

4 Official Response of the BiH Data Protection Agency dated 9 December 2020;

authority has explicitly refused to execute the Agency's orders to remove the respective published data.

However, it should be noted, when it comes to imposing the fines, that such activity is directly dependent upon capacities of the Agency and that they are insufficient in all segments, both human and material. This is particularly relevant because, among other things, issuance of misdemeanour warrants entails other activities as well, such as participation in misdemeanour proceedings which are conducted throughout BiH and for which the presence of the Agency's officials should be ensured, which is difficult due to the aforementioned insufficiency of the Agency's capacities.

This leads us to the next challenge relating to the Agency's imposing the fines in general where it determines violations of the Current Data Protection Law. In this respect, it should be noted that the Agency generally orders administrative measures, and only exceptionally it imposes fines which are extremely low. As an example, in 2019 the Agency issued only 25 fines for violations of provisions of the Current Data Protection Law. The fines issued in 2019 ranged between EUR 150 to EUR 5,000 (while the fines stipulated by the Current Data Protection Law may amount up to EUR 50,000). However, one additional circumstance emphasised by the Agency[5] should be kept in mind in this respect. It refers to the Agency being empowered to either impose a fine directly or to submit a misdemeanour request to the competent court. If it imposes fines directly, it is entitled to impose only minimal penalties. On the other hand, the competent court may, if a misdemeanour request is sent to it, impose a fine of up to its maximum prescribed amount. So far, the Agency has opted for imposing the fines directly (instead of filing misdemeanour requests with the competent courts) and there are two reasons for such position. The first one is that misdemeanour proceedings before courts are lengthy (which raises the question of the protection's effectiveness) and the second one is that, under the current court practice, if data controllers initiate misdemeanour proceedings against orders of the Agency, the courts usually pass decisions by which the sentences are suspended or impose even lower sentences than those imposed by the Agency.

Further, although the Agency conducts supervisions of the data processors/controllers, which usually result in issuing decisions ordering administrative measures, the imposed measures do not affect the data processors/controllers in the expected way.

Specifically, even after complying with the issued administrative measure in a specific case, the entities continuously fail to correct their future actions. In this regard, the entities continue to act in a way that violates the Current Data Protection Law, this being especially pronounced when it comes to the processing of personal ID card number or a copy of ID card, as well as processing of personal data in tender procedures, publication of personal data on official websites (similar to the situation previously described in regard to the publication of name and addresses of persons infected by Covid-19), etc.

Based on the Report on the Protection of Personal Data in BiH for 2019, the Agency conducted only 16 inspections in 2019[6]. From the available information it can be concluded that the filed Data Processing Complaints were mostly related to the potential violation of personal data by public entities, and are mostly related to audio and video surveillance, as well as processing of employee personal data.

Furthermore, 64 Data Processing Complaints were filed in 2019 against data processors/controllers in public sector[7], out of which 22 were determined as founded and were mostly related to audio and video surveillance and processing of the personal ID card number or copy of ID card.

5 Official Response of the BiH Data Protection Agency dated 9 December 2020

6 Report on the Protection of Personal Data in BiH for 2019 dated 27 July 2020, page 14;

7 Report on the Protection of Personal Data in BiH for 2019 dated 27 July 2020, page 17;

Additionally, 69 Data Processing Complaints were filed in 2019 against data processors/controllers in private sector[8] out of which 27 were determined as founded and were also mostly related to audio and video surveillance and unjustified processing of personal data such as ID card number.

As it can be concluded from the aforementioned, the largest number of conducted procedures was related to the processing of personal data through video surveillance, processing of employee personal data, and publication of personal data on websites. Some of the examples are presented below.

One of the cases was a complaint filed by a doctor employed in a health institution. The complaint was related to the processing of personal data through video surveillance in the laboratory of the health institution, more precisely personal data of patients while the very important diagnostic procedures were being carried out in the central laboratory of the health institution. The Agency concluded that such data processing was performed in an unlawful way, and as such is not compliant with the provisions of Current Data Protection Law, which resulted in a removal of installed CCTV cameras in the central laboratory of the health institution.

Complaints regarding video surveillance can be found in almost all annual reports on protection of personal data issued by the Agency to date. In this regard, the Agency issued an official opinion back in 2013 emphasising that, in the case when video surveillance is not legally required, the controller must determine the purpose of its establishment. In addition, one must consider whether the installation of video surveillance is really necessary and whether a different solution would be sufficient for the achievement of the purpose intended. Some examples where introducing video surveillance would be considered as appropriate include protection of company property, specifically, prevention of frequent thefts[9].

In this regard, it is undisputable that the data controllers often have an interest in establishing video surveillance as a necessary technical measure to protect their property. As regards the employees, their data are being collected because they are covered by video surveillance, including for example, their entrance/exit in/from office buildings of the controller, corridors to the warehouses, etc. In this case, the controller must decide on the establishment of surveillance and place the notice on video surveillance in a prominent place and, prior to the establishment, inform employees about the purpose.

However, if the surveillance was introduced solely for the purpose of controlling the work of employees, then, according to the provisions of the Labour Law, the controller can only do so if required by law or to exercise the rights and obligations arising from the employment relationship. Since the legislation of BiH and its Entities contains no regulation that obliges controllers to install video surveillance in the workplace – in offices in which "ordinary" and not some specific work takes place, the controllers have no legal basis for such action. In case of a breach, a fine in the amount of EUR 50,000 may be imposed.

Control of the presence of employees in the workplace may be exercised by other means and fully satisfy the purpose of such processing without unduly encroaching on the privacy of employees. In this aforementioned case the measure ordering deletion of the so far collected fingerprints was issued by the Agency.

Complaints related to the unlawful use of video surveillance were common in 2018 as well. At the request of the Agency to provide information on the installation of video surveillance cameras for the purpose of protecting the fishery fund and preventing poaching by the Sport Fishing Association "Ključ" from Ključ, it stated that it received a donation of one video camera and four cameras, pointing out that the cameras were not put into operation,

8 Report on the Protection of Personal Data in BiH for 2019 dated 27 July 2020, page 18;

9 Official opinion of the BiH Data Protection Agency dated 23 October 2013;

but that there was a great need to set and put them in function in several places where scales and hatcheries are located, which are also tourist attractions[10].

In accordance with the principle of fairness and legality, and according to the relevant legal regulations, it follows that the processing of personal data by video surveillance cameras in public places may be carried out by the Ministry of Internal Affairs for the purpose of conducting police activities to prevent criminal offenses or to maintain order and security.

Watercourses are public places that should be accessible to citizens without any restrictions, except as required by law, and it is unacceptable that they are monitored through video surveillance established by the Society during their stay in these areas. The use of video surveillance cameras in the described manner creates a concern for citizens about privacy threats, which are justified regardless of whether or not the cameras are operational. The Sport Fishing Association was forbidden to process personal data in this way and was ordered to remove video surveillance cameras installed on river watercourses in the municipality of Ključ.

As seen from this case from 2018, the Agency concluded that installation of video surveillance without legal purpose for its installation, regardless of whether or not the installed video surveillance is operational, represents a justifiable threat to the citizens' privacy, and as such is to be considered as unlawful pursuant to the Current Data Protection Law.

However, even with aforementioned official opinion issued by the Agency in 2013, and procedures conducted upon filed complaints related to the unlawful installation of video surveillance evident in almost all annual reports issued by the Agency, entities in both private and public sectors continue to act in the same manner. Repetition of the same actions by private and public entities clearly indicates that the measures taken by the Agency are not sufficient enough.

Furthermore, unlawful publishing of personal data is often subject of complaints filed with the Agency. Acting upon the complaint of the data subject filed against the kindergarten, due to the publication of personal data of children and their parents on the official website of the kindergarten for the purpose of informing parents about those on the waiting list and those whose application for enrolment in the kindergarten was rejected, the Agency rendered the filed complaint as grounded. Consequently, the kindergarten was prohibited from publishing personal data of children and their parents on its official website.

Acting upon the submitted complaint a procedure was initiated against the Central Election Commission of BiH in order to determine the legality of publication of electoral register as a way of delivering the decision rejecting their entry in the central electoral register for voting outside of Bosnia and Herzegovina.

The publication was made on the official website and it was consisted of the list of persons whose applications for entry in the central electoral register for voting outside of BiH were rejected. The published list contains information on the municipality / city, number of applications, name and surname, age, city, deficiency of the application, and the status. The announcement was made for the purpose of delivering the decision on rejection of voting outside of BiH to the applicants.

In the context of the above, it is important to point out that despite the fact that the controlled entities generally carry out the ordered administrative measures imposed by the Agency, and despite the fact that the Agency continuously publishes the respective activities, this does not affect other entities in the expected way (this is especially pronounced when it comes to the processing of personal ID number/a copy of ID card, processing of personal data in tender procedures, publication of personal data on official websites, and similar).

10 Report on the Protection of Personal Data in BiH for 2018 dated 14 May 2019, page 26

In this regard, we should be aware of the fact that the penal policy introduced by the Current Data Protection Law is very mild. It can freely be said that it is symbolic in comparison to the draconian fines imposed by the GDPR.

Considering that, generally speaking, there is also a low level of enforcement, it can easily happen that the level of compliance with the data protection requirements imposed by the Draft Data Protection Law would be as low as it was/is with respect to the Current Data Protection Law.

For the sake of avoiding such scenario – avoiding creation of non-compliance environment as the "normal" state of affairs which does not lead to any actual sanctions or damages regardless of the breaches of the law, the following steps should be undertaken as the priority:

1. Inspection supervision of the Current Data Protection Law should be intensified (to the extent possible considering the existing staff restraints faced by the Agency);
2. Offence proceedings should be initiated without exception against data controllers/processors breaching the law;
3. Public awareness of the data protection importance (in particular when it comes to the rights data subjects have under the Current Data Protection Law) should be further raised (this shall further lead to the more significant reputational risk for data controllers/processors);
4. Capacities of the Agency should further be strengthened;
5. The fact that the Draft Data Protection Law, which is generally aligned with the GDPR, should supersede the Current Data Protection Law in the (relatively) near future, along with the fact that the GDPR, due to its extraterritorial effect, may be fully applicable to local data controllers/processors as well, should be emphasised continuously.

5. CRUCIAL STEPS FOR OVERCOMING THE EXISTING CHALLENGES

In order to avoid creation of non-compliance environmental as the "normal" state of affairs in Bosnia and Herzegovina, which will definitely lead to no actual sanctions or fines to the entities in violation of data protection, significant improvements are needed in the field of data protection. These steps include the intensification of inspection supervision of the Current Data Protection Law, which we believe should be the main priority, raising the public awareness on the importance of data protection, and finally accentuation of the expected adoption of the New Data Protection Law and the extraterritorial effect of the GDPR. Current capacities of the Agency should also be strengthened. Details of these crucial steps are given below:

I. INSPECTION SUPERVISION OF THE CURRENT DATA PROTECTION LAW SHOULD BE INTENSIFIED

Pursuant to the Rulebook on Supervision Inspection Regarding Personal Data Protection, inspection supervision can be initiated by the inspectors on the basis of the approved inspection work plan, upon filed complaint of the data subjects, and upon the order of the Director of the Personal Data Protection Agency in case of suspicion that the provisions of Current Data Protection Law may be breached.

The inspection supervision is performed by (i) undertaking inspection activities to determine the situation in the field of data processing and protection; (ii) determining administrative measures for the purpose of preventing and eliminating illegalities in the implementation of regulations in the field of data processing and protection; and undertaking other measures

and actions determined by the Current Data Protection Law, and relevant secondary legislation.

The supervision inspection makes a direct insight into the legality of work of the controllers and processors, and implementation of administrative measures for prevention and elimination of illegal application of regulations in the area of personal data protection. The supervision inspection also has a preventive purpose to induce discipline in application of regulations in the area of personal data protection.

Supervision activities are conducted by the inspectors. The inspectors have the right and duty to perform direct check of business premises and other facilities for processing of personal data, the work process, personal and other documents. They also perform other activities in line with the purpose of supervision inspection. All data controllers and processors are obliged to enable to inspectors to supervise and look into the required data and materials, to supply necessary information and data of importance for the supervision. The inspectors are obliged to keep confidential all data obtained during the inspection.

While conducting the supervision inspection, the inspectors have the right to directly perform the following:

1. To enter all premises for processing of personal data. Entrance and control of assets and the room of the data controller or processor, which are not provided by the law, may be carried out only during the working hours;
2. To request from the data controller or processor to submit for review any document or records containing personal data, and supply any information on any issue whatsoever upon request;
3. To request from the data controller or processor to terminate illegal processing of personal data, and order other measures which the data controller or processor is obliged to undertake without delay and notify the Agency thereon in written form within 15 days.

If, during the inspection, the inspector determines violations of the applicable legislation, he/she has a right and is obliged to order the following measures:

1. To eliminate the identified deficiencies and irregularities within 15 days;
2. To block, delete or destroy personal data, temporarily or permanently prohibit processing to warn or issue a notice to the controller or processor;
3. To prohibit the processing of personal data that is contrary to the basic principles of lawful processing of personal data and the rights of data subjects;
4. To impose and collect a fine;
5. To take other administrative measures and actions that it deems necessary.

The inspector may also take appropriate preventive activities in order to prevent the occurrence of harmful consequences due to deficiencies and irregularities in the implementation of the Current Data Protection Law, other laws and regulations on the basis of which the processing of personal data is executed, such as:

1. A warning to the controller or processor on the obligations from the above regulations;
2. Pointing out the harmful consequences;
3. Proposing measures to eliminate their causes;
4. Other preventive activities.

Based on the issued Report on the Protection of Personal data in BiH for 2019, it is evident that 16 inspections were conducted in 2019[11], all of which were extraordinary inspections based on Data Processing Complaints or ex officio supervisions mostly connected to processing of data through video surveillance, and processing of employee's personal data.

On the other hand, not a single regular or audit inspection was conducted by the Agency in 2019. According to the Report on the Protection of Personal data in BiH for 2019, the only reason for non-execution of these inspections is the lack of staff, which is a serious problem for the efficiency of the Agency's work.

For the purpose of comparison, the number of inspections conducted in 2019 is the lowest it has been for the previous 9 years. Please find below the table containing statistical information related to the conduced inspections.

Conducted inspections										
Year	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
Number	40	17	99	111	88	90	93	83	42	16

Source: Report on the Protection of Personal Data in BiH for 2019 issued by the Agency

The numbers of inspections need to be much higher due to the importance of inspection supervision for the protection of personal data. It is especially important to increase the number of regular inspections (as noted above, not a single regular inspection was conducted in 2019), having in mind the preventive character of such inspections which would "force" the data processors/controllers to comply with the Current Data Protection Law.

In order to achieve this goal, it is crucial to improve the capacities of the Agency, since the Agency is seriously understaffed as has been continuously emphasised by the Agency for years now.

Specifically, the Rulebook on Internal Organisation of the Agency envisages employment of 45 employees; however currently only 26 employees are employed in the Agency which represents only 57.7% of required capacities of the Agency[12].

Unfortunately, this issue has not been adequately addressed by the competent authorities so far.

II. PUBLIC AWARENESS ON THE DATA PROTECTION IMPORTANCE SHOULD BE FURTHER RAISED

General conclusion is that data protection is still a new term in Bosnia and Herzegovina, consequently the awareness of citizens of BiH about the rights they have under the Current Data Protection Law is still not sufficiently developed.

As an example, in 2019 the Agency received only 133 Data Processing Complaints, which is surely not a result of high compliance with the Current Data Protection Law in BiH, but the direct result of low awareness of data subjects of their rights under the Current Data Protection Law and other relevant legislation.

Therefore, it is necessary to further raise public awareness on the data protection, which primarily needs to done through the work of the Agency as the public authority with primary competences in the field of data protection, e.g. by launching awareness raising campaigns, organising conferences and trainings, and the like.

The aforementioned raising public awareness can be achieved, among other, by data protection training, which could start even in schools, for which purpose the Agency could

11 Report on the Protection of Personal Data in BiH for 2019 dated 27 July 2020

12 Official Response of the BiH Data Protection Agency on our inquiries, dated 29 September 2020

cooperate with the cantonal ministries of education and science in Federation of BiH as well as with the Ministry of Education and Culture of Republika Srpska.

Furthermore, seminars and webinars can be held on various topics related to the data protection, with participation of experts in field of data protection. If conducted, these activities will most likely result in a different approach to the data protection by general public.

For the sake of completeness, the above does not mean that the Agency has not organised any trainings, seminars or lectures so far. On the contrary, various activities of such type have already been undertaken – the Agency held various seminars and lectures especially in the public sector for civil servants, employees of local self-government units, police officers, holders of judicial functions, law students, training in the business sector, etc. It has also held, as described in its annual reports on personal data protection for 2017 and 2018, trainings for school-age children entitled "Do not leave traces on the Internet". Further, in cooperation with the chambers of commerce at the state and entity levels, training sessions were held for businesses, out of which two training sessions in Sarajevo and one in Banja Luka. To the same end, in cooperation with the Association of Banks, training was held for interested legal entities and the banking sector. Two training sessions were also held in cooperation with the American Chamber of Commerce (AmCham) and Banja Luka Business Security Center.

In any case, for the sake of further development in the field of relevant data protection training, employees of the Agency should be further trained and constantly educated as well. In addition, in order to provide concrete answers to the raised questions, and not merely cite relevant legislation, training of the Agency's employees need to be conducted regularly.

For implementation of the aforementioned, the Agency can cooperate with various experts in the field and seek aid when necessary. Generally, cooperation with various experts in the field of data protection as well as in fields related to the data protection would be highly beneficial to the Agency which would consequently improve data protection awareness and finally data protection as well.

Further training should be held for public officials as well, due to the fact that public officials are often involved in non-compliance with the Current Data Protection Law. This is clearly evident from the most recent case involving publication of personal data of persons infected by COVID-19, as well as those subjected to self-isolation, which is in detail described in Chapter II, Section 2 of this report.

Cases mentioned in Section 2 herein clearly suggest that the entities in public sector are often those breaching provisions of the Current Data Protection Law, which most likely happens due to the lack of adequate knowledge in a field of data protection. All that can be improved with sufficient and frequent training provided to public officials.

In 2019 and 2020 the Agency was involved in the following conferences and workshops, on both national and international level[13]:

1. Spring Conference of European Data Protection Authorities – a permanent and the largest conference of European Data Protection Authorities which is held annually since 1991.

   National data protection authority of the economy from which the Chairman of the Conference was elected has the role of the Secretariat of the Conference.

   Bosnia and Herzegovina became a full member of the Spring Conference of European Data Protection Authorities at the Spring Conference held 3-4 May 2012 in Luxembourg.

13 Official Response of the BiH Data Protection Agency on our inquiries, dated 29 September 2020

2. Conference of Central and Eastern European Data Protection Authorities (CEEDPA) - an international forum which enables data protection bodies of Central and Eastern Europe to share their unique experience in the field of data protection.

   This forum was organised in 1991 by economies of Central and Eastern Europe faced with the challenges of accession to the European Community.

   BiH has joined this forum of cooperation as a member at the 14th Conference of CEEDPA-e, held from 20 to 22 May 2012 in Kyiv (Ukraine).

   Meetings were tasked to assist in creating the basis for data protection in local legislation, regulating the status of the bodies that have dealt with it and their powers. Once they become members of the EU, these economies have continued to work on harmonisation of standards in the field of personal data protection and assisting economies in their environment that have faced the challenges of meeting the requirements for membership.

3. Case Handling Workshops – organised twice a year with the aim of training of employees in the national data protection authorities and the exchange of experiences.

4. 10th International Conference "Data protection" Moscow – which was held in November of 2019 in Moscow.

   In addition to the representatives of supervisory bodies and controllers from the Russian Federation, the Conference was attended by representatives of the personal data protection bodies from Jordan, the Kyrgyz Republic, Italy, Azerbaijan, Serbia, Hungary, Morocco, and representatives of international organisations of the European Supervisor and the Council of Europe, executive bodies, the largest controllers of personal data, as well as representatives of expert communities.

   The main part of the Conference on 7 November 2019 covered the following topics: legislative reform in the field of personal data protection (Russia passed a new law and signed the Protocol), improvement and harmonisation of national legislation within the framework of the ratification process of the Protocol, the personal data economy as a key condition in the process of digital economy development, the impact of GDPR in the development of the digital economy, a crucial area for improving legislation in the processing of personal data relating to problem solving and the creation of innovative software solutions in the digital economy, Big Data in the digital economy, the dependence of economic growth of the economy on the correct interpretation of personal data, GDPR applications pan-European approaches, such as non-EU economies, depersonalisation and anonymisation of personal data, methods, requirements, application experience, processing of personal data, balancing operator interests and citizens' rights, and the Internet as a medium for new challenges and threats to privacy.

5. Initiative 2017 - follows the example of similar informal cooperation of the data protection authorities of Nordic states which also share historical, cultural and legal background and which have been closely cooperating and sharing experiences.

   The aim of Initiative 2017 is to join the efforts of all participating supervisory authorities from the region since the authorities face similar challenges and technical issues. Numerous companies and public sector organisations in the region exchange and transfer personal data across borders or boundaries, therefore harmonising the interpretation of data protection standards and guaranteeing effective protection of personal data in the region is an important economic benefit for all the participating economies.

   There was a common agreement among the participants that the initiative in the area of human rights as a model of best practice will greatly benefit the work of all the

participating authorities considering common economical and historical framework and contribute to good relations and cooperation between all the economies in the region.

In addition to all the above stated, it should also be mentioned that the Agency is a permanent member of the Advisory Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, which is the Council of Europe's key body for monitoring the implementation of the Convention. The Agency has also been a member of the International Conference of Data Protection and Privacy Authorities (ICDPPC) since 2011.

Furthermore, the important role of the Agency can be strengthened especially in the eyes of private entities and natural persons, if the public sector sets an example of trust, compliance with the measures, observations, recommendations, opinions and instructions of the Agency and recognition of its independent role.

The aforementioned can be done by frequent publication of the steps taken by the Agency for the purpose of data protection. Even though the Agency publishes its annual reports which outline core problems it faces as well as steps and projects taken in previous year, including materials developed, such as its opinions, decisions and case law, which are all certainly relevant for raising awareness about the importance of personal data protection, further intensification of these activities would be welcomed for further development in the field of data protection.

For the same reason, frequent publications of educational videos, podcasts, articles, and general information on the web page of the Agency, would be useful as well. The Agency can also publish magazine articles, newsletters and write press releases, all in ordered to raise awareness of the general public about data protection.

The Agency can further conduct a study on the level of data protection awareness of the general public. This would offer a clear overview of the current situation, according to which the necessary steps for increasing awareness can be tailored. The Agency should consider publishing articles and other information through a profile on Facebook, Twitter and other communication and social networking platforms used by the general public, since such communication steps would reach many concerned individuals.

The tool that would significantly help in the process of raising awareness in the field of data protection is a platform for questions and answers. This platform, to the best of our knowledge, has not been implemented by public institutions in BiH to this day. However, creation of this platform could be helpful in the process of raising awareness in the field of data protection, especially since the general impression is that data protection is still a new term in Bosnia and Herzegovina and citizens still do not have sufficiently developed awareness of the importance of personal data protection.

The platform should be available to everyone to submit a question to the Agency, which would then be responded and saved on the platform where any interested person could access and search through the data protection questions which are most frequently asked.

Furthermore, it should be noted that implementation of the Draft Data Protection Law will in particular require increased level of data protection awareness.

III. CAPACITIES OF THE AGENCY SHOULD FURTHER BE STRENGTHENED

However, in order to implement all the aforementioned steps, the Agency must have the capacity to perform the assigned duties and responsibilities. At the moment, the Agency does not have the necessary capacities (number of employees, budgets, premises, etc.) in order to legally and efficiently perform the tasks entrusted to it. Activities such as inspection controls, complaints procedures, opinions, issuing misdemeanour orders, participation in court proceedings, maintenance of the Central Registry, etc. are very demanding and imply having sufficient capacities. The Rulebook on internal organisation should also be adopted.

The problem of lack of employees and premises, and insufficient budget was underlined as one of the main challenges in the work of the Agency in their official response to our inquiries. The Agency considers that insufficient number of employees and lack of relevant technical capacities negatively affect the awareness of data controllers and Agency's ability to carry out basic tasks in its competence. This is particularly challenging in conducting inspections, which consequently have negative effect on the awareness of data controllers of the lawful processing of personal data and insufficient knowledge of the relevant legislation which all result in frequent violations of the right to protection of personal data.

According to the provided information, pursuant to the decision of the BiH Council of Ministers, the Agency has the premises of only 308.69 m2. In addition to that, the number of official vehicles should be increased as well[14].

All the above stated should be considered as regards raising public awareness on the importance of adequate data protection. As noted by the Agency[15], raising public awareness in the field of data protection would also entail more citizen complaints, more requests for issuance of the Agency's opinions and more supervisory activities by the Agency, to which the Agency would not be able to respond given its current capacities.

IV. THE FACT THAT THE DRAFT DATA PROTECTION LAW, WHICH IS GENERALLY ALIGNED WITH THE GDPR, SHOULD SUPERSEDE THE CURRENT DATA PROTECTION LAW IN THE (RELATIVELY) NEAR FUTURE, ALONG WITH THE FACT THAT THE GDPR, DUE TO ITS EXTRATERRITORIAL EFFECT, MAY BE FULLY APPLICABLE TO LOCAL DATA CONTROLLERS/PROCESSORS AS WELL, SHOULD BE EMPHASISED CONTINUOUSLY.

Due to its alignment with the GDPR, the Draft Data Protection Law should supersede the Current Data Protection Law in relatively near future.

Although the Draft Data Protection Law represents a copy of the GDPR in its biggest part, in some parts it is still not as strict as the GDPR, but still represents a significant improvement in comparison with the Current Data Protection Law. Specifically, the Draft Data Protection Law introduces fines in the amount of up to BAM 200,000 (approx. EUR 100,000) or 4% of the total worldwide annual turnover of the preceding financial year (whichever is higher), which represents significantly higher fines than those currently applicable pursuant to the Current Data Protection Law.

It is clear that the adoption of GDPR in 2018 had a positive effect on data protection in Bosnia and Herzegovina due to its extended territorial application which was recognised by entities in private sector, mostly larger organisations, which process large amounts of data. Furthermore, it should be continuously emphasised that the GDPR should be, due to its extraterritorial effect, fully applicable to the local data controllers/processors, including small local entities in addition to those with foreign founders and big organisations, and that it is expected that the Draft Protection Law which foresees significantly higher level of protection and penal policy than the Current Data Protection Law should be adopted in the near future. This should result in higher awareness of the data processors and controllers of the importance of data protection, primarily due to the high penal policy of the GDPR and the Draft Data Protection Law, in comparison with the penal policy of the Current Data Protection Law.

14 Official Response of the BiH Data Protection Agency on our inquiries, dated 29 September 2020

15 Official Response of the BiH Data Protection Agency, dated 9 December 2020

The fact that the Draft Data Protection Law should supersede the Current Data Protection Law in the relatively near future may be emphasised as part of the abovementioned public awareness raising campaigns, which should suggest to data controllers to invest in data protection compliance measures and undertake actions in order to achieve compliance with the Draft Data Protection Law.

CHAPTER III. KOSOVO*

1. CURRENT STATUS

The main law governing data protection and privacy in Kosovo* is the Law No. 06/L-082 on Personal Data Protection ("**Current Data Protection Law**"). It superseded the Law No. 03\L-172 on Protection of Personal Data from 2010 ("**Old Data Protection Law**") which was applicable as of May 2010, nearly a decade before the Current Data Protection Law became applicable.

Deficiencies of the Old Data Protection Law were detected in the course of its application and significant improvements were needed (such as, for example, in the field of data transfer regime or legal grounds for data processing). It was also necessary to align the Kosovo* data protection legislation with the new EU data protection regulation – GDPR.

The adoption of the Current Data Protection Law was aimed to serve that purpose. This Law entered into force on 10 March 2019.

The Current Data Protection Law represents a copy of the GDPR in its biggest part. Nevertheless, certain differences do exist, whereas the most obvious one is the stricter regulation in terms of data transfer regulations (as detailed below under item 8 of Section 2) and somewhat milder penal policy (as detailed below under item 9 of Section 2.).

Other than this, it should be noted that the Current Data Protection Law does not envisage any of the recitals introduced by the GDPR (it contains 173 recitals) and, thus, lacks explanations as a very important tool for its full understanding and adequate application.

The overview of the most important rules governed by the Current Data Protection Law, compared with the relevant GDPR rules, follows below in Section 2. The relevant secondary legislation will also be covered by the respective overview.

The authority competent for data protection matters in Kosovo* is the Information and Privacy Agency ("**Agency**"). The Agency is seated in Prishtina and its official website is https://aip.rks-gov.net.

The Agency was established by the Current Data Protection Law, replacing the Agency for Protection of Personal Data (which was established under the Old Data Protection Law) as the authority with the exclusive competence in the field of protection of personal data.

Due to the recent adoption of the Current Data Protection Law and the vast number of prescribed obligations, the current enforcement of the Current Data Protection Law is low. One of the main and most important challenges in the implementation of the Current Data Protection Law in Kosovo* is the institutional vacuum left considering that the old Agency for Protection of Personal Data (which was established under the Old Data Protection Law) is no longer operational, while the new Agency is not fully operational, as the Commissioner of the Agency has not been appointed yet.

The capacities and proper establishment of the Agency seem to be amongst the most problematic aspects in terms of the introduction and enforcement of the Current Data Protection Law. Amongst other issues, the Current Data Protection Law provides a six-month timeframe for the Agency to enact the new secondary legislation. Although such deadline has passed, the Agency is yet to enact the respective bylaws based on the Current Data Protection Law.

The Agency still seems not to be at its full working capacity since the Agency Commissioner is yet to be elected. As such, the first and most important step going forward is for the Agency to gain full working capacity and start enacting bylaws, strategies, guidelines as

well as to start proper supervision and inspection of data control compliance on the market. Moreover, the Agency needs to become more transparent and have publicly available reports, documents and data on their official website.

In any case, further information on the Agency and the challenges faced in its work is provided in Section 3 bellow.

2. ASSESSMENT OF THE LEVEL OF COMPLIANCE OF THE DATA PROTECTION LAW AND RELEVANT SECONDARY LEGISLATION WITH GDPR

As noted above, the Current Data Protection Law is the copy of the GDPR in its biggest part. Therefore, the rules introduced by the respective Law are generally aligned with the GDPR, subject to certain exceptions (e.g. the aforementioned lack of the stringent penal policy envisaged by the GDPR).

This overview contains summary of the most important rules and areas governed by the Current Data Protection Law, as well as identification of the most important secondary legislation and matters stipulated by such legislation, as follows: (1) general data processing requirements, (2) obligations and responsibility of data controllers and data processors, (3) conditions for consent, (4) joint controllers, (5) data processors, (6) data protection officers and representatives of foreign entities, (7) special categories of personal data, (8) rights of data subjects, (9) personal data safety, (10) records of processing activities, (11) data breach related notification and data protection impact assessment, (12) data transfer, (13) means of complaint, liability and penal policy, and (14) relevant secondary legislation.

1. GENERAL DATA PROCESSING REQUIREMENTS

Under the Current Data Protection Law, all personal data, regardless of their type, category of data subjects and scope of a particular processing, should be processed in line with certain processing principles explicitly governed by the respective Law, as follows: (1) personal data should be processed for specified, explicit and legitimate purposes, (2) processing should be carried out lawfully (i.e. should be based on adequate legal grounds), fairly and transparently in relation to the data subjects, (3) processing should be limited to data which is necessary for fulfilling its legitimate purpose(s), (4) processed data should be accurate and, where necessary, kept up to date, (5) processed data should not be retained longer than necessary for the purpose(s) for which they are processed, (6) processing should be performed in a manner that ensures appropriate security of the processes data.

The Current Data Protection Law provides for the following principles of personal data processing:

1. Principle of lawfulness, justice and transparency – personal data are processed in an impartial, lawful and transparent manner, without infringing the dignity of data subjects.
2. Principle of purpose limitation – data are collected only for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered as incompatible with the initial purpose.
3. Principle of data minimisation – personal data shall be adequate, relevant and limited to the purposes for which they are further collected or processed.
4. Principle of accuracy – personal data shall be accurate and kept up to date; every reasonable step must be taken to ensure that personal data which are inaccurate, as regards the purposes for which they are processed, are erased or rectified without delay.
5. Principle of storage limitation - personal data may be stored insofar as necessary to achieve the purpose for which they are further collected or processed. After the fulfilment of processing purpose, personal data shall be erased, deleted, destroyed, blocked or anonymised, unless otherwise foreseen by the Law on State Archives or by another relevant law.
6. Principle of integrity and confidentiality – personal data shall be processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
7. Principle of accountability – the controller shall be responsible for, and be able to demonstrate compliance with all principles set forth.

As indicated above, the requirement of carrying out the data processing lawfully means that, amongst other, it should be based on adequate legal grounds. Such legal grounds include:

1. If the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
2. If processing is necessary for the performance of a contract to which the data subject is a contracting party or in order to take steps at the request of the data subject prior to entering into a contract;
3. If processing is necessary for compliance with a legal obligation which the controller is subject to;
4. If processing is necessary in order to protect the vital interests of the data subject or of another natural person;
5. If 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; or
6. If 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. This shall not apply to the processing carried out by public authorities in the performance of their tasks (jointly "**Statutory Grounds**").

Based on the above, it is clear that, other that consent, all other Statutory Grounds include necessity of a particular data processing to be achieving a specific legitimate purpose(s).

The respective legal grounds correspond to the data processing legal grounds envisaged by the GDPR (Article 6).

Moreover, all data processing requirements identified above are fully aligned with the data processing principles envisaged by the GDPR (Article 5).

2. OBLIGATIONS AND RESPONSIBILITY OF DATA CONTROLLERS AND DATA PROCESSORS

Data controllers and data processors are obliged to process data in compliance with all the data processing principles described above. There is also the obligation to be able to demonstrate the respective compliance (accountability).

This should be done by implementing appropriate technical, organisational and human resources measures, whereas the nature, scope, context and purposes of the particular processing, as well as the risks of varying likelihood and severity to the rights and freedoms

of natural persons, should be taken into consideration. The measures should ensure adequate protection of the processed data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. The rights of data subjects should be duly protected.

The measures should be reviewed and updated where necessary and, if proportionate in relation to processing activities, they should also include the implementation of appropriate data protection policies.

The same as the GDPR, the Current Data Protection Law does not prescribe the exhaustive list of the respective measures, but solely provides some examples (such as pseudonymisation and encryption) and in general describes their purpose and circumstances to be taken into consideration when deciding on their implementation.

When it comes to the relationship between a data controller and a data processor, a written data processing agreement of the prescribed content should be entered into between them. This agreement should govern relevant characteristics of a particular processing (such as the nature and purpose of the processing, its subject matter and duration, type(s) of processed data and category(ies) of data subjects) and mutual rights and obligations of the parties (e.g. obligation of a data processor to process the data only according to the controller's documented instructions, to ensure that the persons authorised to process personal data are obliged to keep data confidentiality, etc.).

Further, a data controller should only engage a data processor which provides sufficient guarantees that the appropriate measures shall be undertaken in such a way that the processing shall meet statutory requirements and that the protection of the data subject rights shall be ensured. It is also explicitly envisaged that a processor should not engage another processor (i.e. sub-processor) without prior written authorisation, general or specific, of the data controller.

Considering the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity to the rights and freedoms of natural persons, the data controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the Current Data Protection Law. Those measures shall be reviewed and updated where necessary.

Taking into account the state of technology, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity to rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of 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 Current Data Protection Law and protect the rights of data subjects.

The data controller shall implement appropriate technical and organisational measures to ensure 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. In particular, such measures shall ensure that by default personal data are not made accessible to an indefinite number of natural persons without the individual's intervention.

Further obligations of data controllers and/or data processors are described n item 3 and items 5-8 of this Section 2.

3. CONDITIONS FOR CONSENT

In line with the Current Data Protection Law, if processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to process his or her personal data.

If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from other matters, in an intelligible and easily accessible form, using clear and plain language.

The data subject is entitled to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. The withdrawal shall be done in the same way as giving of the consent.

When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on the consent to the processing of personal data that is not necessary for the performance of that contract.

The Current Data Protection Law prescribes that processing of personal data of a child shall be lawful where the data subject has given consent to the processing of his or her personal data for one or more specific purposes with regard to providing the information society services directly to the child, and where the child is at least sixteen (16) years old. When the child is under the age of sixteen (16), such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.

The controller shall make a reasonable effort to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.

If data processing is made for children aged below sixteen (16) to fourteen (14), data controller shall make continuous efforts to verify if in such cases the consent is actually given or authorised by parents or the custodian, taking into consideration the available technology.

4. JOINT CONTROLLERS

If two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall transparently determine their respective responsibilities for compliance with the obligations under the Current Data Protection Law, in particular as regards exercising the rights of the data subject and their respective duties to provide the information, by means of an arrangement between them. The arrangement may designate a contact point for data subjects.

Such arrangement shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects. The essence of the arrangement shall be made available to the data subject.

Irrespective of the terms of the arrangement, the data subject may exercise his or her rights under the Current Data Protection Law in respect of and against each of the controller.

5. DATA PROCESSORS

If processing is to be carried out on behalf of a controller, 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 Current Data Protection Law and ensure the protection of the rights of the data subject.

The data processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

Processing by a processor shall be governed by a contract that is binding on the processor with regard to the controller and that 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. This contract shall stipulate, in particular, that the processor:

1. Processes personal data only according to documented instructions from the controller, including with regard to transfers of personal data to a foreign economy or an international organisation, unless required to do so by a special law which the processor is subject to; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest. The processor shall immediately inform the controller if, according to his/her opinion, a certain rule is in contradiction with the Current Data Protection Law;
2. Ensures that persons authorised to process personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
3. Takes all measures regarding safety of processing required under the Current Data Protection Law;
4. Uses only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the Current Data Protection Law and ensures protection of the rights of data subject;
5. Does not engage another processor without prior specific or general written authorisation of the controller;
6. Considering the nature of the processing, assists the controller with appropriate technical and organisational measures, insofar as this is possible, for fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights;
7. Assists the data controller in ensuring compliance with the obligations under the Current Data Protection Law considering the nature of processing and the information available to the processor;
8. At the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Law on Archives requires storage of data;
9. Makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in the Current Data Protection Law and allows for and contributes to the audits, including inspections, to be conducted by the controller or another auditor mandated by the controller.

If a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor shall be imposed on that other processor by way of a contract or other legal act under applicable legislation, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the Current Data Protection Law. If that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.

The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by any specific law.

6. DATA PROTECTION OFFICERS AND REPRESENTATIVES OF FOREIGN ENTITIES

The controller and the processor shall designate a data protection officer in any case where:

1. The processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
2. 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; or
3. The core activities of the controller or the processor consist of processing on a large scale of special categories of data and personal data relating to criminal convictions and offences.

A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.

Where the controller or the processor is a public authority or body, a single data protection officer may be designated for several such authorities or bodies, taking account of their organisational structure and size.

Otherwise, the controller or processor or associations and other bodies representing categories of controllers or processors may voluntarily designate a data protection officer. The data protection officer may act for such associations and other bodies representing controllers or processor.

The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks provided by the Current Data Protection Law.

The data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract.

The controller or the processor shall publish the contact details of the data protection officer and communicate them to the Agency.

The controller and the processor shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data. The controller and processor shall support the data protection officer in performing their tasks by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.

The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing his or her tasks. The data protection officer shall directly report to the highest management level of the controller or the processor.

Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under the Current Data Protection Law.

The data protection officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks. The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.

When it comes to representatives of foreign entities, it should be noted that the Current Data Protection Law recognises the respective representatives, but the concept of their appointment (i.e. of the circumstances which lead to such appointment) differs from the respective GDPR concept (due to the fact that, unlike the GDPR, the Current Data Protection Law envisages the location of the data processing equipment as the crucial circumstance for determining whether the respective appointment is obligatory or not).

Specifically, the Current Data Protection Law envisages that foreign entities, i.e. data controllers and processors which are not established on Kosovo* territory, but which use automatic or other equipment located in this economy for data processing purposes, have to designate their representatives in Kosovo*, unless the respective equipment is used only for purposes of transit through the economy's territory. This representative can be either a natural person or legal entity, but it has to be available as the respective foreign entity's contact point in Kosovo* to both the Agency and local data subjects.

7. SPECIAL CATEGORIES OF PERSONAL DATA

The definition and further rules on processing of these personal data, as prescribed by the Current Data Protection Law, correspond to the respective GDPR rules.

Specifically, special categories of personal data include data revealing racial or ethnic origin, political opinion, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health and data concerning a natural person's sex life or sexual orientation. In comparison with the Old Data Protection Law (which recognised the so-called particularly sensitive data), biometric and genetic data are completely new types of personal data which were not governed by the Old Data Protection Law at all.

Generally, any processing of special categories of data is prohibited. However, this is not an absolute prohibition, i.e. their processing is allowed in certain exceptional cases explicitly prescribed by both the Current Data Protection Law and GDPR (Article 9) ("**Exceptional Cases**").

Specifically, the Exceptional Cases are the following cases:

1. The data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where the relevant legislation in force provide that the respective data processing prohibition may not be lifted by the data subject;
2. Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by the relevant legislation in force or a collective agreement providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
3. Processing is necessary to protect vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
4. Processing is carried out in the course of legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to their members or data subjects who have regular contact with it in connection with its purposes and that the personal data are not disclosed without the consent of the data subjects;
5. If the data subject has made them public without limiting their use in an evidenced or clear manner;
6. Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
7. Processing is necessary for reasons of substantial public interest, on the basis of relevant legislation;
8. Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of relevant legislation or pursuant to contracts with a health professional when such data are processed by a professional or under his/her responsibility subject to the obligation of professional secrecy pursuant to respective legislation, established rules by competent bodies or by another person subjected to professional secrecy;
9. Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border/boundary threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of relevant legislation;
10. Processing is necessary for achieving purposes in the public interest, scientific or historical research purposes or statistical purposes.

Accordingly, only the processing which "fits in" one of the Exceptional Cases can be regarded as allowed processing of special categories of personal data. Otherwise, a general prohibition of their processing is applicable.

In addition, the following rules on processing of biometric data should also be taken into consideration:

1. The public sector may use biometric features only if this is necessary and required for the safety of people, the security of property or the protection of confidential data and business secrets, under condition that this cannot be achieved by milder means or that this is compliant with obligations arising from binding international agreements, or for the identification of persons crossing territorial boundary;
2. The private sector may use biometric features only if this is necessary and required for the performance of activities for the safety of people, the security of property or the protection of confidential data or business secrets. Employees must be informed in writing prior to the use of their biometric characteristics about the intended measures and their rights. In any case, data controllers may implement measures using biometrics only after the receipt of an authorisation from the Agency.

8. RIGHTS OF DATA SUBJECTS

The Current Data Protection Law envisages a set of rights which belong to data subjects in relation to their personal data's processing. Exercise of these rights may be conditioned upon fulfilment of certain requirements and/or may be limited depending on the circumstances of each particular case. The law explicitly governs such requirements/limitations as well ("**Prescribed Restrictions**").

In general, subject to the Prescribed Restrictions, these are the following rights:

1. Right to request information on a particular processing;
2. Right to access the processed data and obtain their copy;
3. Right to rectification of the processed data;

4. Right to erasure (*right to be forgotten*);
5. Right to restriction of the data processing (e.g. if the processed data's accuracy is contested by the data subject);
6. Right to data portability (i.e. right to receive the processed data from the data controller in a structured, commonly used and machine-readable format, as well as to transmit them or to have them transmitted from one controller to the other);
7. Right to object to the data processing (e.g. if the processing is based on the legitimate interest or performed for direct marketing purposes) and to the processing's cessation;
8. Right to withdraw consent (where consent is a legal ground for processing), and
9. Right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning the data subject or significantly affects him/her ("**Relevant Rights**").

The majority of Relevant Rights have already been recognised by the Old Data Protection Law, but some of them are completely new (e.g. right to data portability). In any case, data controllers are obliged to ensure exercise of the Relevant Rights (subject to the Prescribed Restrictions) and to do so within exact terms explicitly prescribed by the Current Data Protection Law (i.e. within 30-day period/up to 90-day period if extension of 60 days is necessary due to complexity and number of the requests for the exercise of respective rights). If they fail to fulfil their statutory obligation or comply with the relevant timeline, data subjects are entitled to file a complaint with the Agency ("**Data Processing Complaint**").

Also, any person who considers that any of his/her rights were infringed by processing activities of a data controller/processor is entitled to the court protection of his/her rights.

If the purposes for which a controller processes personal data do not or no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with the Current Data Protection Law.

Where the controller is able to demonstrate that it is not in a position to identify the data subject, the controller shall inform the data subject accordingly, if possible. In such cases, rights of access by data subject as well as rights to data portability shall not apply except where the data subject, for the purpose of exercising his or her rights under those articles, provides additional information enabling his or her identification.

The above-described concept of the respective rights is aligned with the GDPR (Chapter III – Rights of the data subject).

9. PERSONAL DATA SAFETY

Considering the technology, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity to the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

1. The pseudonymisation and encryption of personal data;
2. The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
3. The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
4. A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

In assessing the appropriate level of security, accompanying risks shall be considered in particular the risks that are presented by processing, particularly from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

Adherence to an approved code of conduct or an approved certification may be used as an element by which to demonstrate compliance with the safety of processing requirements.

The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by any specific law.

Personal data processing may be entrusted to a data processor under a written contract, to conduct such operations pursuant to procedures and security measures.

Data processor may act only within the constraints of the authorisations given by data controller and is not entitled to process personal data for other purposes. Mutual rights and obligations should be specified by a written contract, which should also contain a detailed description of procedures and measures in accordance with the Current Data Protection Law.

Data controllers should oversee implementation of procedures and measures in accordance with the Current Data Protection Law. They should also conduct periodical visits to the premises where personal data are processed.

In case of a dispute between the data controller and processor, the latter should immediately, upon controller's request, return all the data in possession. The data processor is not allowed to keep copies of data and further process them.

In case of discontinuation of data processor's activity, personal data shall immediately be returned to the data controller.

The data protection officer shall have at least the following tasks:

1. To inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to the Current Data Processing Law and to secondary legislation on data protection;
2. To provide advice, where requested, as regards the data protection impact assessment and monitor its performance pursuant to the Current Data Processing Law;
3. To cooperate with the Agency;
4. To act as the contact point for the Agency on issues relating to processing, including the prior consultation, and to consult, where appropriate, with regard to any other matter.

The data protection officer shall, in the performance of his or her tasks, have due regard to the risk associated with processing operations, considering the nature, scope, context and purposes of processing.

10. RECORDS OF PROCESSING ACTIVITIES

The obligation imposed by both the Current Data Protection Law and GDPR is the obligation of data controllers and data processors to keep records of their data processing activities.

These records should be established in a written form (including also electronic form). They should be kept permanently and should be made available to the Agency upon its request.

Their content is explicitly prescribed. Specifically, the following information on the processing should be included in these records:

1. Name and contact information of the controller and where applicable, of the common controller, the representative of the controller and the DPO;
2. Purpose of processing;
3. A description of data subject categories and personal data types;
4. Categories of recipients to whom personal data were or shall be disclosed, including recipients in third economies or international organisations;
5. Data on transfer of personal data to third economies or to an international organisation, where applicable;
6. Where possible, the envisaged time limits for erasure of the different categories of data;
7. Where possible, a general description of technical and organisational security measures.

However, this obligation exists only if data controllers/processors have at least 250 employees or, regardless of their employee number, if the processing is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data or personal data relating to criminal convictions and offences.

Although the Current Data Protection Law imposes the above-described obligation of keeping records of processing activities, it does not oblige data controllers to register their databases containing personal data with the Agency, as it was the case with the Old Data Protection Law.

11. DATA BREACH RELATED NOTIFICATION AND DATA PROTECTION IMPACT ASSESSMENT

Both the obligations regarding data breach related notifications and data protection impact assessment are novelties introduced by the Current Data Protection Law in line with the GDPR. None of them was envisaged by the Old Data Protection Law.

The fulfilment of these obligations depends on the fact whether a particular processing (or a data breach) is likely to result in a risk or high risk to the rights and freedoms of natural persons. If such risk would exist in a particular case, a data controller would be obliged to act as follows: (1) to notify (without undue delay or, if possible, within 72 hours) the Agency and/or data subject of a particular data breach (e.g. if an unauthorised person has accessed the processed personal data and made them available to general public), and (2) to carry out the assessment of an impact which a particular processing could have on the protection of personal data, prior to commencing such processing, whereas it is prescribed that the Agency shall establish and publish a list of the processing operations for which this assessment is required ("**Obligatory Assessment List**"). In this regard, it should be noted that the Obligatory Assessment List has not yet been enacted and published by the Agency.

Also, when it comes to a data breach, a data processor is obliged to notify a data controller of a data breach without undue delay after becoming aware of the same.

a. *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 seventy-two (72) hours after having become aware of it, notify the personal data breach to the Agency, 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 seventy-two (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.

The notification to the Agency shall at least:

1. Describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
2. Communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
3. Describe the likely consequences of the personal data breach;
4. Describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the Agency to verify compliance of the controller.

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

The communication to the data subject shall describe in clear and plain language the nature of the personal data breach.

The communication to the data subject shall not be required if any of the following conditions are met:

1. The controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
2. The controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise;
3. It would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

If the controller has not already communicated the personal data breach to the data subject, the Agency, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so.

b. *Data Protection Impact Assessment*

Where a type of processing in particular using new technologies, and considering 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 risk.

The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.

A data protection impact assessment shall in particular be required in the case of:

1. 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;
2. Processing on a large scale of special categories of data, or of personal data relating to criminal convictions and offences; or
3. A systematic monitoring of a publicly accessible area on a large scale.

The Agency shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment. The Agency may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required.

The assessment shall contain at least:

1. A systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
2. An assessment of the necessity and proportionality of the processing operations in relation to the purposes;
3. An assessment of the risks to the rights and freedoms of data subjects; and
4. The measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the Current Data Protection Law considering the rights and legitimate interests of data subjects and other persons concerned.

Compliance with approved codes of conduct by relevant controllers or processors shall be taken into due account in assessing the impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment.

Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.

Where processing has a legal basis in any specific law to which the controller is subject, that law regulates the specific processing operation or set of operations in question, and a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis, data protection impact assessment requirements shall not apply, unless the Agency considers it necessary to carry out such an assessment prior to processing activities.

Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.

The controller shall consult the Agency prior to processing if a data protection impact assessment indicates that the processing would result in a high 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 Current Data Protection Law, particularly if the controller has insufficiently identified or mitigated the risk, the Agency shall, within period of up to 8 weeks of receipt of the request for consultation, provide a written advice to the controller and, where applicable, to the processor. That period may be extended for 6 weeks, considering the complexity of the intended processing. The Agency shall inform the controller and, where applicable, the processor, of any such extension within one (1) week of receipt of the request for consultation together with the reasons for the delay. Those periods may be suspended until the Agency has obtained information it has requested for the purposes of the consultation.

When consulting the Agency, the controller shall provide the Agency with:

1. Where applicable, the respective responsibilities of the controller, joint controllers and processors involved in the processing, in particular for processing within a group of undertakings;
2. The purposes and means of the intended processing;
3. The measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to the Current Data Protection Law;
4. Where applicable, the contact details of the data protection officer;
5. The data protection impact assessment; and
6. Any other information requested by the Agency.

Notwithstanding the above, the Agency may require controllers to consult with, and obtain prior authorisation in relation to processing for the performance of a task in the public interest, including processing in relation to social protection and public health.

12. DATA TRANSFER

Personal data transfers to other jurisdictions may take place only in the following cases:

1. If the transfer is to be made to a jurisdiction with an adequate level of data protection. To this end, the Agency determines and publishes the list of economies pertinent to this group;
2. If authorised by the Agency (if the transfer is to be made to an economy without adequate level of data protection) (“**Transfer Approval**”).

a. *Adequate Level List/Decisions*

The transfer to other economies and international organisations of personal data that are processed or are intended to be processed after the transfer may take place only in accordance with the provisions of the Current Data Protection Law and if the economy or the international organisation in question ensures an adequate level of data protection.

Economies and international organisations are considered as ensuring an adequate level of data protection if the Agency has taken a formal decision and they are included in the respective list established by the Agency in accordance with the Current Data Protection Law.

The Agency shall maintain a list of economies and international organisation or one or more sectors specified within them for which it finds that they ensure an adequate level of data protection.

In order to draft a list, the Agency may apply decisions taken by a competent body of the EU on whether such economies and international organisations provide an adequate level of data protection.

The Agency shall publish the list of economies and international organisations that ensure an adequate level of data protection in the Official Gazette and on its website.

In its decision-making on the adequate level of protection of personal data of another economy or an international organisation, the Agency shall determine all circumstances relating to the transfer of personal data. In particular by considering the following elements:

1. The rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectorial, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third economy or international organisation which apply within that economy or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;
2. The existence and effective functioning of one or more independent supervisory authorities in the third economy or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities;
3. The international commitments the third economy or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data;
4. The type of personal data to be processed;
5. The purpose and duration of the proposed processing;
6. The legal arrangement in the economy of origin and the recipient economy, including legal arrangement for protection of personal data of foreign citizens;
7. The measures to secure personal data used in such economies and international organisations.

In its decision-making, the Agency shall, in particular, take account of:

1. Whether the personal data to be transferred will be or are used solely for the purpose for which they are transferred, or whether the purpose may change only on the basis of a permission of the data controller supplying the data or on the basis of personal consent of the data subject;
2. Whether the data subject has the possibility of determining the purpose for which his or her personal data will be or have been used, to whom they are or were supplied and the possibility of correcting or erasing inaccurate or outdated personal data, unless this is prevented due to the secrecy of the procedure by binding international treaties;
3. Whether the foreign data controller or data processor performs adequate organisational and technical procedures and measures to protect personal data;
4. Whether there is an assigned contact person authorised to provide information to the data subject or to the Agency on the processing of personal data transferred;
5. Whether the foreign data recipient may further transfer personal data only on the condition that another foreign data recipient to whom personal data will be disclosed ensures adequate protection of personal data also for foreign citizens;
6. Whether effective legal protection is ensured for data subjects whose personal data were or are to be transferred.

The Agency shall carry out a periodic review of the list, at least every four (4) years, which shall consider all relevant developments in the third economy or international organisation that could affect the permanence in the list.

The Agency shall, where available information reveals that a third economy, one or more specified sectors within a third economy, or an international organisation no longer ensures an adequate level of protection, to the extent necessary, amend or suspend the decision of inclusion in the list by means of implementing acts without retroactive effect.

The Agency shall, by a bylaw, define in greater detail which information is necessary to decide whether another economy or an international organisation provides an adequate level of data protection for the purpose of the Current Data Protection Law.

b. *Transfer Approval*

The Agency issues the Transfer Approval if one or more of the following conditions are met:

1. It is so provided by another law or binding international treaty;
2. The data subject has given consent and is aware of the consequences of the transfer;
3. The transfer is necessary for the performance of a contract between the data subject and the data controller or for the implementation of pre-contractual measures taken in response to the data subject's requests;
4. The transfer is necessary for the conclusion or performance of a contract concluded in the data subject's interests between the data controller and a third party;
5. The transfer is necessary and legally required on the grounds of important public interest;
6. The transfer is necessary to protect the life and body of the data subject;
7. The transfer is necessary for the establishment, exercise or defence of legal claims;
8. The transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, to the extent that the conditions laid down for consultation are fulfilled in this particular case. In this case, the transfer shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. Where the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients; or
9. The data controller adduces adequate safeguards for the protection of personal data and the fundamental rights and freedoms of individuals as regards the exercise of corresponding rights. Such safeguards may result from the provisions of the contract or the general terms of business activities governing the transfer of personal data.

The data controller may transfer personal data only upon receipt of the authorisation. In his or her request for authorisation the data controller shall provide the Agency with all information necessary regarding the required transfer of personal data. This includes in particular the categories of data, the purpose of the transfer and the safeguards in place for the protection of personal data in the other economy or international organisation.

The Agency shall decide on the application without delay and shall define in a bylaw the details and internal procedures for filing such requests. The abovementioned decision is final in administrative procedure but an administrative dispute shall be permitted before the competent court.

The authorisations concerning the transfer of personal data to another economy or international organisation granted by the Agency shall be registered in accordance with the processing activity records requirements provided by the Current Data Protection Law.

Judgements and any decision of a third economy administrative authorities requiring transfer or disclosure of personal data by controllers or processors can only be recognised or implemented based on the international agreement between the third economy submitting the request and Kosovo*, without prejudice to the reasons for transfer under the Current Data Protection Law.

13. MEANS OF COMPLAINT, LIABILITY AND PENAL POLICY

One of the most noticeable differences between the Current Data Protection Law and the GDPR is probably the penal policy.

The Current Data Protection Law provides, as a general rule and for most offences, a penalty of up to EUR 40,000 for the breaching entity and up to EUR 2,000 for its responsible person. As an exception, the Current Data Protection Law provides for penalties of up to 4% of the general turnover of the previous fiscal year (in line with the GDPR) for situations in which the Agency determines a serious and great violation of personal data. The terms "serious" and "great" are not defined so it is left to the Agency's interpretation to assess and determine when to impose such sanctions.

In comparison, the Old Data Protection Law provided for much lighter penalties ranging up to EUR 10,000 for the breaching entity and up to EUR 2,000 for its responsible person.

Without prejudice to other administrative or judicial remedies of protection, any data subject has the right to file a complaint before the Agency, if the data subject claims that the processing of his or her personal data violates the Current Data Protection Law.

The Agency shall notify the complainant of the progress and outcome of the complaint, including the possibility of a judicial remedy.

Without prejudice to any other administrative or non-judicial remedy, each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of the Agency concerning them.

Without prejudice to any other administrative or non-judicial remedy, each data subject shall have the right to an effective judicial remedy where the Agency, based on its powers, does not address a complaint or fails to notify the data subject within three (3) months on the progress or outcome of the complaint lodged pursuant to the Current Data Protection Law. The unsatisfied party has the right to initiate an administrative dispute before the competent court against Commissioner's final decision.

Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under the Current Data Protection Law have been infringed as a result of the processing of his or her personal data in non-compliance with the Current Data Protection Law.

The data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law in force, as statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf, to exercise rights on his or her behalf, and to exercise the right to receive compensation on his or her behalf.

The authorisation for the representative must be given in writing and certified by the competent body.

Any person who has suffered material or non-material damage as a result of an infringement of the Current Data Protection Law shall have the right to receive compensation from the controller or processor for the damage suffered.

Any controller involved in processing shall be liable for the damage caused by processing which infringes the Current Data Protection Law. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of the Current Data Protection Law specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.

A controller or processor shall be exempt from liability if it proves that it is not in any way responsible for the event giving rise to the damage.

Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject.

Where a controller or processor has paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage, in accordance with the Current Data Protection Law.

For the compensation of the damage the party is entitled to file a lawsuit before the competent court.

14. RELEVANT SECONDARY LEGISLATION

The Current Data Protection Law provides a six-month timeframe for the Agency to enact the new secondary legislation. Although such deadline has passed, the Agency is yet to enact the respective bylaws based on the Current Data Protection Law.

The secondary legislation acts currently in force were all issued prior to the new Current Data Protection Law entering into the force. However, as long as they do not contradict the Current Data Protection Law, they will remain in force until the issuance of the new secondary legislation acts.

According to the information provided by Mr. Valon Kryeziu, Director of Agency Legal Department, the Agency has started drafting some of the respective secondary legislation acts. However, an expected timeframe as to when the acts can be expected to be enacted was not provided.

The following acts are still in force:

1. Regulation no. 01/2015 dated 23 January 2015 on the manner of storage and use of archive material and protocol ("**Storage Regulation**"). The Storage Regulation was adopted by the now defunct Agency for Protection of Personal Data. The Storage Regulation sets out the methodology, procedures and conditions for the documents which are received in the archive of the Agency for Protection of Personal Data and the way the same are received, delivered, stored, classified and reproduced. Any material which is received for archiving is stored as a whole, in the condition in which the relevant unit received it. The same cannot be alienated, damaged or destroyed. Completed materials are marked on the cover, archived and registered in the archive book. When storing the archive material electronically, whether on servers or other electronic devices, a high security system must be applied to protect the material from unauthorised access and potential risks of cybercrime. Additionally, all material which is stored electronically must have a physical copy stored separately from the basic data, in accordance with the standards for data storage information technology. The Storage Regulation was adopted before the GDPR was published and is thus not in line with the GDPR;
2. Regulation no. 03/2015 dated 7 May 2015 on security measures in the course of personal data processing, as amended;
3. Regulation no. 05/2015 dated 23 June 2015 on the manner of registering in the records of databases and the pertinent record forms; and
4. Decision of the Agency Council no. 02/09 dated 22 April 2016 on the economies with an adequate level of protection for personal data, as amended – which lists the

following economies as having adequate level of personal data protection: Austria; Latvia; Belgium; Lithuania; Bulgaria; Luxembourg; Croatia; Malta; Cyprus; Finland; Czech Republic; Poland; Denmark; Portugal; Estonia; Romania; Finland; Slovakia; France; Slovenia; Germany; Spain; Greece; Sweden; Hungary; Great Britain; Republic of Ireland; Israel; Liechtenstein; Norway; Switzerland; Argentina; Australia; Andorra; Canada; Guernsey; Isle of Man; Jersey; Faroe Islands and New Zealand.

3. COMPETENCE OF AND CHALLENGES IN THE WORK OF THE AGENCY

The public authority with the competence in the field of data protection is the Information and Privacy Agency (in Albanian, *Agjencia për Informim dhe Privatësi,* in Serbian: *Agencija za informacije i privatnost*).

The Agency is an autonomous public authority established in 2019. Under the Current Data Protection Law, in fulfilling its duties and exercising its powers the Agency acts free of external influence, whether direct or indirect, and does not solicit or receive instructions from anyone.

The Current Data Protection Law stipulates that the Agency is to be led by the Commissioner. The Commissioner shall be elected by the Kosovo* Assembly with a majority of votes of the total number of Parliament members for a five-year mandate with the right to be re-elected for another mandate. To the best of our knowledge, the Agency's Commissioner is yet to be elected by the Kosovo* Assembly.

The Agency is financed from the budget of Kosovo* and it has its own budgetary line which should guarantee its independence. The Agency is obliged to submit an annual activity report on its work to the Kosovo* Assembly and to publish it, not later than by 31 March each year for the previous calendar year.

The Agency's competences are set in detail by the Current Data Protection Law. Amongst other, the Agency is to undertake the following activities:

1. Supervises the implementation of the Current Data Protection Law;
2. Provides advice to public and private bodies on issues related to data protection;
3. Informs the public on issues and developments in the area of data protection;
4. Promotes and supports fundamental rights to personal data protection;
5. Decides about complaints submitted by data subjects;
6. Provides advice to the Assembly, the Government, other internal institutions and bodies on legislative and administrative measures in relation to protection of fundamental rights and freedoms of natural persons in terms of data processing;
7. Carries out inspections regarding the implementation of the Current Data Protection Law.

For the purpose of exercising the authorisations and duties within its sphere of competence, the Agency basically has two types of powers:

1. Powers relating to its capacity of a second-instance authority responsible for protecting the right to data protection in appeal proceedings (i.e. based on the Data Processing Complaints filed with the Agency) ("**Appeal Related Powers**"), and
2. Powers relating to its capacity of a supervisory authority responsible for enforcing the Current Data Protection Law ("**Supervisory Powers**").

When it comes to the Agency's Appeal Related Powers, it decides on filed complaints within 30 days from the day of their filing, whereas it firstly forwards the complaints to the data controller(s) responsible for undertaking data processing activities which the complaints were filed against for their comments. Depending on whether the Agency finds a complaint grounded, it may reject it (if ungrounded) or order the data controller to act upon the request within a specified period of time (if grounded). In any case, no appeal can be filed against a decision passed by the Agency, but an administrative dispute can be initiated against such decision (or if the Agency does not pass a decision within the statutory term) before the competent court.

When it comes to the Agency's Supervisory Powers, the Agency is entitled, amongst other, to order certain corrective measures to data controllers/processors (e.g. to order them to stop undertaking particular data processing activities), as well as to file a request for initiating offence proceedings against them before the competent court. Additionally, the Current Data Protection Law also establishes the Agency's competence to issue fines for all offences directly based on the Current Data Protection Law.

As detailed above, the Agency's scope of work and authorisations are rather broad. As we were informed by Mr. Valon Kryeziu, Director of Agency Legal Department, one of the main challenges the Agency currently faces is the need for further capacity building and human resources to cover such broad scope of work and authorisations.

Furthermore, Mr. Kryeziu also confirmed that the Agency is currently not involved or participating in any projects. However, they do expect a twinning IPA 2 project to start at the beginning of 2021. Mr. Kryeziu has also expressed the Agency's openness and interest to be part of projects that would help the Agency in its development and capacity building.

In addition to the Agency, other relevant institutions in the data protection area include, but are not limited to:

1. **Kosovo* Assembly** - The Kosovo* Assembly is the legislative authority of Kosovo*. It is the authority which adopts the laws in the economy, and as such has adopted the Current Data Protection Law. The Agency is accountable for its work to the Assembly and prepares and submits annual reports about its work to the Assembly. The Assembly also appoints and dismisses the Commissioner of the Agency. Additionally, the Assembly is the only body competent for interpreting laws in Kosovo* by issuing an authentic interpretation.
2. **Ministry of Justice of Kosovo*** - The Ministry of Justice is one of the key players involved in drafting new legislation and harmonising economy's legislation with the acquis communautaire.
3. **Basic Courts** - The basic courts in Kosovo* are the judicial authority which decides in first instance in damage claims proceedings. Moreover, the Basic Court Administrative Matters Departments are responsible for the first instance of administrative conflicts based on lawsuits filed against final administrative acts (such as those of the Agency).
4. **Constitutional Court of Kosovo*** - The Constitutional Court is the authority which protects the constitutionality and legality and the rights and freedoms of individuals. It is the authority which decides whether the adopted laws and regulations are in line with the Kosovo* Constitution. Anyone can submit an initiative to the Constitutional Court to initiate a procedure for assessing the constitutionality of the Current Data Protection Law, or any of its provisions, and whether they are legal and in line with the Constitution of Kosovo*.
5. **State Prosecution Office** - The State Prosecution Office is the authority that prosecutes perpetrators of crimes, including crimes related to data protection (e.g. abuse of personal data). The State Prosecution Office can be aided by different bodies, e.g. the police (in certain situations the police would aid the Agency as well), etc.

4. CHALLENGES IN THE IMPLEMENTATION OF THE CURRENT DATA PROTECTION LAW IN PRIVATE AND PUBLIC SECTOR

One of the main and most important challenges in the implementation of the Current Data Protection Law in Kosovo* is the institutional vacuum left considering that the old Agency for Protection of Personal Data (which was established under the Old Data Protection Law) is no longer operational, while the new Agency is not fully operational.

The Agency has not become fully operational yet because the Commissioner of the Agency has not been appointed yet. As mentioned above in Section 3 of this Chapter III, the Kosovo* Assembly is the authority which is competent for appointing the Commissioner of the Agency.

The fact that the Commissioner has not been appointed yet causes organisational and functional problems for the Agency's work since the organisation and internal functioning of the Agency should be regulated by a bylaw which should be enacted by the Commissioner. Also, some of the matters governed by the Current Data Protection Law cannot be implemented yet since the Agency has still not adopted the relevant bylaws.

On the other hand, there are also numerous other challenges faced by local entities in both private and public sector in Kosovo*. The most important ones include the following:

1. Burdensome statutory requirements with respect to internal acts, decisions, etc. required in order to be fully compliant with the Current Data Protection Law;
2. Lack of understanding and knowledge on the market with respect to the compliance requirements;
3. Challenges linked to the full and adequate implementation of the data processing principles envisaged by the Current Data Protection Law, in particular the principle of accountability and data protection by design and default.

The most demanding of the above is to implement the above-identified principles introduced by the Current Data Protection Law.

This is due to the fact that the implementation of respective principles requires from the entities involved in any processing of personal data to respect the data protection requirements (such as, for example, data minimisation) from the very creation/further development of their IT system as, otherwise, they would not be able to respond to or address the challenges which the respective law imposes (such as, for example, the requirement to ensure exercise of the data subject processing rights and to ensure such exercise is made within the terms envisaged by the law, or requirement to timely prepare and file data breach notifications).

Accordingly, full and adequate implementation of the Current Data Protection Law requires significant investments (e.g. for obtaining adequate equipment/software and hiring qualified personnel) by the vast majority of the respective entities.

The data minimisation principle should also be mentioned. Its application may be challenging in practice, considering that various types of records/registries are, presumably, kept by the local processing entities, containing much personal data, whereas not all of them are absolutely necessary for the achievement of their legitimate processing purposes. Minimising the retention terms whenever possible will be a challenge of its own.

Also, the level of public awareness when it comes to importance of personal data protection and knowledge of the rights of individuals as data subjects is rather low as well.

Generally speaking, there is also a low level of enforcement, which is why it can easily happen that the level of compliance with the data protection requirements imposed by the Current Data Protection Law would be as low as it was with respect to the Old Data Protection Law.

Considering such circumstances, local data controllers and data processors (to which significant obligations are imposed by the Current Data Protection Law) may ask themselves why to invest resources and efforts in reaching full compliance with the respective law, if there would be no or at least no significant consequences for their non-compliance.

Before providing information on the crucial steps (Section 6 of this Chapter III) to be undertaken for the sake of avoiding such scenario – for avoiding that the environment of non-compliance would become/remain the "normal" state of affairs which does not lead (and/or is not perceived to lead) to any actual fines, other sanctions or any other relevant consequences regardless of the breaches of the law which may have been committed, the attention should be paid to the appointment of the Commissioner of the Agency. As already mentioned above, the vacant position of the Commissioner is an obstacle for the Agency to become fully operational and, thus, obstacle for further development of local data protection law and environment as well.

In the end, before going into details regarding selection of the Agency Commissioner (Section 5 of this Chapter III), it should also be mentioned that the occurrence and spread of Covid-19 in the world and in Kosovo* slowed down the process of implementation of the Current Data Protection Law, which was enacted right at the time of outbreak. The Agency, as well as other institutions, worked in reduced capacity for several months. Generally, the availability of the Agency should improve in the forthcoming period.

5. CRITERIA AND PROCEDURE FOR SELECTING THE COMMISSIONER

The candidates for the Commissioner of the Agency should fulfil the specified criteria in order to be selected and certain procedure before the Kosovo* Assembly as the authority competent for electing the Commissioner should be followed. Further information on both the criteria and procedure follow below.

1. COMMISSIONER SELECTION CRITERIA

Candidates for the Commissioner must meet the following criteria:

1. To be a citizen of Kosovo*;
2. To have a university degree in one of the following fields: law, public administration or international relations;
3. Should have at least eight (8) years of professional experience, of which at least five (5) years of experience in managing positions;
4. Should not have been convicted by a final decision for a criminal offense or should have no indictment for the last five (5) years;
5. Must have high moral and professional integrity;
6. Should have experience and distinguished knowledge in the area of human rights protection;
7. Should not have been dismissed from work or civil service due to a disciplinary measure;
8. Should not have exercise any function in any political party during past five (5) year;
9. Should not be a member of the Assembly of the Legislature of the Kosovo* Assembly which elects him/her, or a member of the Government Office in the last mandate.

2. COMMISSIONER SELECTION PROCEDURE

The Commissioner shall be elected by the Kosovo* Assembly with a majority of votes of the total number of Members of Parliament for a five-year mandate with the right to be re-elected for another mandate.

The election procedure commences by announcing the job vacancy for the Commissioner's position, which shall be published in mass media, both written and electronic. The job vacancy announcement sets out the criteria for the selection of the Commissioner as provided by the Current Data Protection Law. The vacancy should be open for at least 15 and no longer than 20 days.

After the closing date, the selection panel appointed by the parliamentary committee for security of Kosovo* Assembly within 15 days evaluates if the candidates meet the criteria to be elected as the Commissioner.

The selection panel conducts an interview with each candidate that meets the eligibility criteria and according to the submitted data and the interview results, it prepares a shortlist of candidates qualified to be voted by the Kosovo* Assembly.

The shortlist is composed of 3 candidates, except in the case when there are more candidates with equal points. The selection panel submits the short list to the committee, which proposes the same to the Kosovo* Assembly. The proposal given by the committee contains the justification as to reasons the panel has given priority to some of the candidates compared to the other.

In case of the end of the term of office, the Commissioner exercises his/her function until a new Commissioner is elected.

6. CRUCIAL STEPS FOR OVERCOMING THE EXISTING CHALLENGES

As already mentioned in Chapter III, Section 4 herein, creation of non-compliance environment as the "normal" state of affairs which does not lead (and/or is not perceived to lead) to any actual fines, other sanctions or any other relevant consequences regardless of the breaches of the law which may have been committed, needs to be avoided.

For such purpose, the following steps should be taken as the priority:

1. The Agency's Commissioner should be appointed in the shortest possible term and the Agency should adopt a set of subordinate legislation and additional documents, and also engage in the development of additional mechanisms, all for the sake of enabling full implementation of the Current Data Protection Law and further development of the local data protection environment in general;
2. Harmonisation of the sector legislation with the terms and requirements imposed by the Current Data Protection Law should be carried out;
3. Public awareness of the data protection importance (in particular when it comes to the rights subjects have under the Current Data Protection Law) should be further raised (this shall further lead to the more significant reputational risk for data controllers/processors);
4. Regular and continuous education and training of individuals involved in the processing of personal data both in the public and private sector, including also continuous education of the Agency's staff, should be performed;
5. Inspection supervision of the Current Data Protection Law should be intensified (to the extent possible considering the existing staff restraints faced by the Agency);
6. Offence proceedings should be initiated without exception against data controllers/processors breaching the law;
7. The fact that the Current Data Protection Law is generally aligned with the GDPR along with the fact that GDPR, due to its extraterritorial effect, may be fully applicable to local data controllers/processors as well, should be emphasised continuously.

Further details regarding the above crucial steps for overcoming the most important challenges for further development of local data protection law and practice, and measures covered, are provided below.

- Considering that no further development of local data protection law and environment is possible/realistic to happen before the Agency becomes fully operational, its Commissioner should be appointed as soon as possible, but as also already mentioned above, the Agency should focus on **adopting bylaws to further regulate certain matters envisaged by the Current Data Protection Law**, such as:
  1. Procedures for securing standardised icons and identifying the information to be represented as standardised icons;
  2. Rulebook on keeping the registry of approved codes of conduct;
  3. Standards and norms for accreditation of a body for monitoring the compliance of the codes of conduct;
  4. Certification standards and norms for personal data protection and accreditation of certification bodies;
  5. Rulebook on keeping the registry of all certification mechanisms, as well as data protection seals and marks, etc.
- The Agency should also adopt **standard contractual clauses** to be concluded between data controllers and data processors, standard contractual clauses to be concluded between data transferors and data recipients in case of cross-border/boundary transfer of personal data and **adequacy decisions for third economies**.

  We advise that experts are involved in the process of adoption of the above-mentioned acts and documents, especially GDPR experts which will ensure that the essence of the GDPR is transposed into these documents.
- In addition to the above, it is highly advisable that the Agency develops **additional documents and mechanisms** to make the implementation of the Current Data Protection Law easier and more understandable for data controllers, data processors, data subjects and third parties.

  Particularly, the Agency can develop guidelines on different topics, good practice documents, various templates, handbooks, check lists, etc.

  We would advise that the manuals and guidelines are developed to cover matters which are not explicitly regulated (for example, which internal data protection acts must be adopted by data controllers and data processors, guidance on controllers that have an obligation to appoint a DPO, etc.).

  The Agency can also issue guidelines on how to apply the Current Data Protection Law to specific areas, such as technological developments, health-related data processing at times of pandemics, blockchain and artificial intelligence, etc.
- When it comes to the **harmonisation of the sector legislation with the Current Data Protection Law**, a study could be prepared in order to approach the harmonisation in the best manner possible, while the Agency should be consulted throughout the entire process of this harmonisation and should issue opinions on the draft laws and bylaws

regarding their level of harmonisation with the Current Data Protection Law prior to the draft laws and bylaws being accepted and proposed by the relevant institutions which need to adopt them.

The Ministry of Justice and other competent authorities should initiate the process for transposing of the Directive (EU) 2016/680 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 by competent authorities for the purpose of law enforcement. This should provide a regulatory framework for personal data processing by the police and other law-enforcement authorities.

A special project for aiding the implementation of the Current Data Protection Law by SMEs, as well as charitable organisations and associations, can be implemented, where they would be provided with templates and other practical tools, as well as trainings and grants for data protection compliance.

When it comes to the data portability right and the lack of its implementation in practice, a project can be introduced and implemented so that innovative solutions are designed and created which would enable provision of data in a machine-readable format and allow data subjects to switch between service providers (for example, mobile applications for data management and transfer, tools for providing and withdrawing consent, tools for requesting access to the personal information, etc.).

Having in mind the increased number of IT companies in Kosovo* in the last few years and their fast expansion, as well as the vast amount of personal data which they could encounter in their regular business, we find that the Agency should also focus on the IT companies and their compliance with the Current Data Protection Law.

- **Raising awareness of general public** is absolutely necessary for further development of the local data protection law and environment.

The Agency should work on raising awareness about personal data protection (for example, media workers must be trained on how to make a balance between the protection of personal data and freedom of expression and information) and obligations of data controllers and data processors, and on designing mechanisms and tools which would enable greater availability and access for concerned private entities.

The Agency can publish educational videos, podcasts, articles, and general information on its web page. It can also publish magazine articles, newsletters and write press releases.

Awareness of the population can be raised through data protection training, which should start even in schools, for which purpose the Agency could cooperate with the Ministry of Education, Science and Technology of Kosovo*. Seminars and webinars on different data protection topics can be held, inviting experts in this field.

A platform for questions and answers could be developed where anyone can submit a question to the Agency, which would then respond to the question and the questions and answers on each topic would be saved on the platform where any interested person could access them and search through the data protection questions most frequently posed. This tool would significantly help the implementation of the Current Data Protection Law as it would save time and resources, as well as free the Agency from receiving constant questions referring to the same subject matter. This would also provide more transparency and ensure equal treatment of parties.

The Agency's officials and representatives could intensify their media appearance and discuss different topics, especially hot topics which would draw the attention of general public, such as abuse of personal data online, fake profiles, hacking accounts, video surveillance, etc. The Agency can have open days to promote its work.

The Agency should also consider publishing articles and other information through a profile on Facebook, Twitter and other communication and social networking platforms used by the general public, since such communication steps would reach many concerned individuals.

It would be beneficial if the Agency would frequently publish the steps it is undertaking, relevant investigations and inspections which are taking place, as well as the results of these investigations and inspections. Efforts should be made to ensure impartial and independent work of the Agency through distance supervision and electronic means, as much as possible.

- **Overall transparency and proactive approach of the Agency** are of crucial importance not only for raising the level of public awareness and further education of the public, but also for strengthening the trust of the public in the Agency itself.

The Agency can also conduct a **study on the level of data protection awareness** of the general public. This would offer a clear overview of the current situation, according to which the necessary steps for increasing awareness can be tailored.

Further, the Agency should ensure that every data protection officer (DPO) has undertaken data protection training and should undertake steps to strengthen the position of DPOs, such as further develop the DPO network and encourage its use and the use of all available tools developed by the Agency and available to DPOs.

- **Continuous education of the Agency employees** is of utmost importance as well. They should be trained and educated on how to respond to questions from interested entities and natural persons regarding the implementation of the Current Data Protection Law, especially to provide concrete answers and not merely cite laws, as well as to give particular and practical examples.

Additional investments in the Agency employees should be made in terms of salary increase, and professional advancement and employee training. The Agency can cooperate with various experts in the field and seek assistance when necessary.

The Agency's inspection capacities should be strengthened as well.

- Furthermore, the important role of the Agency can be strengthened especially in the eyes of entities and natural persons, if the **public sector** sets an example of trust, compliance with the measures, observations, recommendations, opinions and instructions of the Agency and recognition of its independent role in Kosovo*.

Training and data protection education sessions should be held for public officials and employees in public institutions in order to raise their awareness and approach to data protection matters.

The general perception is that data protection matters are not taken seriously by public institutions processing vast amount of personal data.

- As already mentioned in Section 4, one of the main challenges when it comes to implementation of the Current Data Protection Law is the low level of enforcement. One of the most important steps to be undertaken is to intensify Agency **inspection supervision** activities and initiate **misdemeanour procedures** if it determines that the Current Data Protection Law was violated, **without exceptions and in a fair and transparent way**. This, however, does not exclude the provision of advice and support for achieving compliance with the Current Data Protection Law, which the Agency should provide to local data processing entities including both data controllers and data processors.

The judges dealing with data protection matters should also be trained and educated on the Current Data Protection Law as well as on the GDPR and its principles, in order to ensure proper and effective judicial protection.

- On the other hand, **local data processing entities** themselves should invest in **data protection compliance measures** and undertake actions in order to achieve compliance with the Current Data Protection Law as soon as possible.

  It is advisable that data controllers perform an internal due diligence on their established data protection system and especially: identify all personal databases and the risks from processing the identified personal data, analyse the status of the appointed DPO and the DPO's independence, assess which technical and organisational measures need to be updated/amended/enhanced, re-evaluate their data processors and review the agreements with the data processors, establish or re-assess the system for data protection training of their employees, review the cross-border/boundary transfers of personal data and their compliance with the Current Data Protection Law, perform internal and external data protection controls, etc.

  It is also advisable that data controllers prepare an action plan on their compliance with the Current Data Protection Law.

- It should be constantly emphasised that the **GDPR** itself may be fully applicable to local data controllers/processors due to its **extraterritorial effect**. Establishing an active cooperation with other data protection authorities, especially in the European Union is advisable. This can also be achieved by the Agency taking active participation in international events and forums, as well as participating and taking initiatives for joint activities with data protection authorities from other economies.

Finally, special attention should be paid to the spread of the Covid-19 in Kosovo*. As previously mentioned in Chapter III, Section 4, it has already significantly influenced the process of implementation of the Current Data Protection Law.

Due to the fast spread and easy transmission of the virus, it became one of the biggest threats to human life and health, as well as businesses and the economy in 2020. This especially impacted the business processes of large companies employing many employees, as some of them had to cease their work, while others even closed down their companies.

Realising that the Coronavirus will be here for some time and that employers need to adapt to the new situation, they became creative in ensuring that the number of employees infected with the virus is brought to a minimum. In addition to other protective measures which employers undertake, they started using advanced technology, some of which raises data protection concerns, as well as large-scale data processing. Furthermore, revealing personal data of employees which are infected with Covid-19 is also questionable. Data protection concerns caused by the Coronavirus spread in other areas, such as education, media, health system, etc. Even though it is undisputed that the right to human life and health prevails, it is of crucial importance to keep the data protection rights to the highest level possible.

Coronavirus may not disappear easily or very soon, hence it is highly recommended that the Agency devotes its attention to achieving a high standard of data protection during the pandemic in Kosovo*. This can be done by preparing guidelines on how to deal with the pandemic from a data protection perspective, advising public authorities and data controllers directly, preparing and publishing opinions on whether certain technologies and monitoring fulfil the data protection requirements, and performing supervisions.

CHAPTER IV. MONTENEGRO

1. CURRENT STATUS

The main law governing data protection and privacy in Montenegro is the Law on Protection of Personal Data (Official Journal of Montenegro, nos. 79/2008, 70/2009, 44/2012 and 22/2017) ("**Current Data Protection Law**").

The Current Data Protection Law was enacted in December 2008 and its last amendments (a few changes of non-substantial nature) were made in April 2017.

For the sake of harmonising the Montenegrin legislation with the General Data Protection Regulation (GDPR), a new data protection law should be adopted. However, although a draft has already been developed and was expected to be adopted by the end of 2019, it has not been enacted yet.

According to the e-mail communication with the relevant government authorities in the course of September 2020, the respective draft was sent to the European Commission, which provided its comments and suggestions that were accepted by the Working Group for the Law and further feedback from the expert from Slovenia is expected. However, we were told that the Working Group could not wait for the respective feedback anymore (due to the current pandemics) and that it intends to provide the revised version of the Draft Law to the European Commission. Upon obtaining its opinion, the Proposed Law will be sent to the Montenegrin Government. It is further expected that the Proposed Law will be sent to the Parliament by the Government and that Parliament will adopt the new law.

It remains to be seen when such adoption will happen, i.e. whether this will occur in the course of 2021. No information in this regard has been published on the website of the Montenegrin data protection authority.

For now, considering that the Current Data Protection Law is still in force, it should be noted that, although the GDPR alignment is yet to come, this does not mean that the rules prescribed by the Current Data Protection Law contradict the GDPR's data processing principles, on the contrary.

In this respect, the overview of most important rules of the Current Data Protection Law against the relevant GDPR rules follows in Section 2 of this Chapter IV. The related secondary legislation is also covered.

The authority competent for data protection matters in Montenegro is the Agency for Personal Data Protection and Free Access to Information ("**Agency**"). The Agency is seated in Podgorica and its official website is www.azlp.me

The Agency was established by the Current Data Protection Law as the authority with the exclusive competence both in the field of protection of personal data and in the field of free access to information, i.e. implementation of the right of the public to know/have access to the information held by public authorities which they have a justified interest to know. This is why the full name of the Agency includes both free access to information and protection of personal data, as identified above.

There was no such authority in Montenegro prior to Agency's establishment. This means that, at the moment, the Agency has more than a decade of experience in the field of data protection. Nevertheless, further improvements are needed, in particular to deal with the issues of the staff insufficiency, necessary intensification of the inspection supervision and too low level of enforcement activities. Further education and raising awareness on data protection importance is of utmost importance as well.

Further information on the Agency, its operation, competences and challenges it faces in its work in the field of personal data protection is provided in Section 3 below.

The last two sections of Chapter IV of this report (Section 4 and Section 5) deal with the most important challenges in Montenegro in terms of further development of data protection law and practice, as well as identification and description of the steps/measures which are/should be of crucial importance for achieving the respective objective.

2. ASSESSMENT OF THE LEVEL OF COMPLIANCE OF THE DATA PROTECTION LAW AND RELEVANT SECONDARY LEGISLATION WITH GDPR

As noted above, the Current Data Protection Law originates from 2008 and, as such, it should not be regarded as the GDPR aligned law. However, as also noted above, this does not mean that its rules are not compliant with the GDPR's data processing principles, on the contrary, such compliance exists at least to a certain extent.

Therefore, the purpose of this overview is to provide a summary of the most important rules and areas governed by the Current Data Protection Law, identify most important secondary legislation and matters prescribed by such legislation, and indicate whether such rules can be regarded as generally compliant with the relevant GDPR rules.

Accordingly, the topics covered by this overview are as follows: (1) general data processing requirements, (2) obligations and responsibility of data controllers and data processors, (3) data protection officers and representatives of foreign entities, (4) special categories of personal data, (5) rights of data subjects, (6) registration and records of processing activities, (7) data breach related notification and data protection impact assessment, (8) data transfer, (9) penal policy, and (10) relevant secondary legislation.

1. GENERAL DATA PROCESSING REQUIREMENTS

Under the Current Data Protection Law, all personal data, regardless of their type, category of data subjects and scope of a particular processing, should be processed in line with certain processing principles explicitly governed by the respective law, as follows:

1. Processed data should be accurate and complete and have to be updated;
2. Processing should be carried out fairly and lawfully;
3. Unless prescribed by a law, a data controller determines the purpose and manner of data processing, or specified, explicit and legitimate purposes;
4. Processing should be limited to data which is necessary for fulfilment of the legitimate purpose(s) of processing;
5. Unless a retention period is prescribed by law, processed data should not be retained longer than necessary for the purpose(s) for which they are processed;
6. Processing should be performed in a manner that ensures the appropriate security of processes data.

Accordingly, although the Current Data Protection Law is not a GDRP aligned law, all the above principles are generally compliant with the GDPR – they are not contrary to any of the processing principles envisaged by the GDPR ("**GDPR Principles**").

In any case, one of the explicitly prescribed requirements is that data processing should be carried out lawfully. This means, amongst other, that it should be based on adequate legal grounds. Such legal grounds is either data subject's consent (which should be a prior informed consent for a particular processing purpose) or one of the remaining grounds explicitly prescribed by the Current Data Protection Law.

Specifically, these grounds include:

1. Necessity of a particular processing for the performance of a contract to which a data subject is party or for the sake of undertaking actions at the request of the data subject prior to entering into a contract;
2. Necessity for fulfilment of the data controller's statutory obligations;
3. Necessity for the protection of life and other vital interests of the data subject who is not able to consent to the respective processing personally;
4. Necessity for undertaking activities of public interest or for exercising the official authority within the scope of work – competence of the data controller, a third party or data user; and
5. Necessity to serve an interest of the data controller, a third party or a data user, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data ("**Statutory Grounds**").

Considering the types/nature of all above-described legal grounds for data processing activities and the fact that each of the Statutory Grounds includes necessity of a particular data processing to achieve specific legitimate purpose(s), it is evident that the respective legal grounds, subject to certain specifics (e.g. the wording "interest based on a law" instead of the GDPR's wording "legitimate interest"), generally correspond to the data processing legal grounds envisaged by the GDPR (Article 6).

The same goes for the above-identified data processing requirements in comparison to the GDPR Principles. Nevertheless, it needs to be emphasised that some of the most important GDPR Principles are not part of the Current Data Protection Law, at least they are not governed in an explicit manner as this is done by the GDPR.

Such principles are (1) the accountability principle (i.e. obligation of data controllers/processors to be able to demonstrate that their processing activities are compliant with the law), (2) principle of data protection by design and by default (i.e. obligation of data controllers/processors to consider data processing principles when designing their data processing systems and to incorporate the respective principles as the respective systems' standard/default mechanisms) and (3) transparency principle (i.e. obligation of data controllers/processor to perform their processing operations transparently towards data subjects).

As a conclusion, rules of the Current Data Protection Law which govern legal grounds for data processing activities, as well as those which govern data processing requirements/principles, generally correspond to the respective rules envisaged by the GDPR, subject to the above-specified exceptions.

2. OBLIGATIONS AND RESPONSIBILITY OF DATA CONTROLLERS AND DATA PROCESSORS

Data controllers and data processors are obliged to perform data processing in compliance with all the data processing principles described above.

For this reason, they should implement appropriate technical, organisational and human resources measures, whereas such measures should correspond to the nature and character of the processed data and state of art technology and costs of its implementation should be taken into consideration. The measures should ensure protection of the processed data

against loss, destruction, unauthorised access, change, publishing and misuse. Neither examples nor exhaustive list of the respective measures are prescribed by the Current Data Protection Law.

Further, data controllers are obliged to:

1. Determine which of their employees are allowed to access the processed data (and which of the respective data);
2. Determine which types of the processed data may be provided to third parties as data users (and under which conditions), and
3. Ensure, if data are processed electronically, that certain information on the respective processing is automatically recorded in their IT systems (e.g. information on the users of the respective data, types of such data, time of log-in and log-out, etc.).

When it comes to the relationship between a data controller and a data processor, a written agreement should be entered into between them. This agreement should govern mutual rights and obligations of the parties, in particular the processor's obligation to act only upon the controller's instructions.

Further, a data controller should only engage a data processor that fulfils conditions for implementing appropriate technical, organisational and human resources measures for the protection of the processed data. It is also explicitly envisaged that a processor should, upon the processing completion, delete the processed data or return them to the data controller.

None of the above rules contradicts the relevant GDPR provisions, but they are not as detailed as the respective provisions. For example, although a written agreement between a data controller and a data processor is envisaged as obligatory by the Current Data Protection Law, no obligatory content of such agreement is prescribed or the rule that a data processor should not engage another processor (i.e. sub-processor) without prior written authorisation, general or specific, of the data controller.

Specifically, the GDPR (Article 28) prescribes that the contract between a data controller and data processor should, in particular, stipulate that the processor: (1) processes the personal data only on documented instructions from the controller, (2) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality, (3) takes all required security measures, (4) respects the conditions for engaging another processor (i.e. sub-processor), (5) taking into account the nature of the processing, assists the data controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the data controller's obligation to respond to requests for exercising the data subject's rights, (6) assists the data controller in ensuring compliance with the obligations regarding security of processing, as well as regarding data breach notifications and data protection impact assessment, (7) at the choice of the data controller, deletes or returns all the personal data to the data controller after the end of the provision of services relating to processing, and deletes existing copies unless storage of the personal data is required by law, (8) makes available to the data controller all information necessary to demonstrate compliance with its obligations and allows for and contributes to audits, including inspections, conducted by the data controller or another auditor mandated by the controller.

It is also prescribed by the GDPR (and not by the Current Data Protection Law) that where the other processor (i.e. sub-processor) fails to fulfil its data protection obligations, the initial data processor (i.e. the one which has entered into an agreement directly with the data controller) shall remain fully liable to the data controller for the performance of that other processor's (i.e. sub-processor's) obligations. Further obligations of data controllers and/or data processors are described in item 3 and items 5-8 of this Section 2.

Considering all the above, it can be concluded that the respective rules of the Current Data Protection Law are not as detailed as the rules envisaged by the GDPR, but are generally compliant with the relevant GDPR rules.

3. DATA PROTECTION OFFICERS AND REPRESENTATIVES OF FOREIGN ENTITIES

Under the Current Data Protection Law, data controllers are obliged to appoint a data protection officer ("**DPO**") if they have at least 10 employees involved in the processing of personal data.

This means that the number of data controller's employees is the sole criterion based on which it is determined whether this obligation exists – whether a data controller is obliged to fulfil it. In other words, neither the types of the processed data nor the nature/purpose of the data processing activities is relevant for existence of the respective obligation and this is the crucial difference in comparison to the GDPR rules on the DPO appointment.

Under the respective GDPR rules (Article 37), the DPO appointment is obligatory in the following 3 cases (in all other cases, it is fully voluntary):

1. The processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
2. The core activities of the data controller or the data 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;
3. The core activities of the data controller or the data processor consist of processing on a large scale of special categories of personal data and personal data relating to criminal convictions and offences.

Additionally, unlike the GDPR, which governs the DPO appointment obligation as the obligation of both data controllers and data processors, the Current Data Protection Law keeps it "reserved" for data controllers only.

Considering the above-stated rules on the DPO appointment governed by the Current Data Protection Law on one side and GDPR on the other, it can be concluded that the respective rules envisaged by the Current Data Protection Law are not compliant with the DPO related rules prescribed by the GDPR.

When it comes to representatives of foreign entities, the GDPR rules also differ from the rules envisaged by the Current Data Protection Law. More precisely, the concept envisaged by the Current Data Protection Law is entirely different from the concept of the respective representative appointment under the GDPR.

Specifically, it is governed by the GDPR (Article 3) that it applies to the processing of personal data of data subjects who are in the European Union even if such processing is carried out by a data controller or data processor not established in the EU, as long as the respective processing activities are related to (1) the offering of goods or services to the data subjects who are in the EU, irrespective of whether a payment of the data subject is required, or to (2) the monitoring of their behaviour as far as their behaviour takes place within the EU.

Accordingly, the above-described extraterritorial effect of the GDPR does not depend on the place where the equipment used for the respective data processing is located (i.e. whether it is within or outside of the EU). On the other hand, the location of the data processing equipment location is crucial under the Current Data Protection Law. Specifically, it is prescribed that if a foreign entity uses the equipment located on the Montenegrin territory for a particular data processing, it is obliged to appoint a local natural person or a legal entity as its representative (or an agent) in Montenegro, unless such equipment is used solely to transfer data over the Montenegrin territory.

It should also be noted that, again differently compared to the GDPR, the obligation of appointing respective representative is prescribed solely for foreign data controllers (i.e. foreign data processors remain out of its scope).

4. SPECIAL CATEGORIES OF PERSONAL DATA

The Current Data Protection Law recognises special categories of personal data and special rules of their processing in a sense that their processing, unless in a few explicitly prescribed cases, is prohibited. In this respect, we can say that the Current Data Protection Law is aligned with the respective GDPR rules (Article 9).

However, such alignment exists only to a certain extent. Specifically, the definition of special categories of personal data envisaged by the Current Data Protection Law does not include all types of personal data which are covered by the respective GDPR definition.

Under the GDPR, special categories of personal data include data revealing racial or ethnic origin, political opinion, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health and data concerning a natural person's sex life or sexual orientation.

On the other hand, the Current Data Protection Law governs that special categories of personal data are personal data relating to racial or ethnic origin, political opinion, religious or philosophical beliefs, trade union membership, as well as data concerning health condition or sex life.

When we compare these two definitions, we can conclude that the Current Data Protection Law does not include biometric data, genetic data and data concerning a natural person's sexual orientation.

In this respect, it should be noted that the Current Data Protection Law does recognise biometric data in that it defines them and governs their processing regime, however it does not include such data in the special categories of personal data, but rather governs their processing as one of the so-called special cases of data processing. In addition to biometric data processing, the remaining of the respective special cases of data processing are (1) video-surveillance, and (2) records of entering/leaving business or official premises.

When it comes to the aforementioned definition of biometric data, as envisaged by the Current Data Protection Law, they are defined as data relating to physical or physiological characteristics of a natural person which are specific, unique and unchangeable and on the basis of which it is possible to determine, directly or indirectly, a natural person's identity.

With regard to biometric data processing regime, as also governed by the Current Data Protection Law, the following is prescribed:

1. It is allowed to determine and compare a person's characteristics for the purpose of determining and proving such person's identity, by processing biometric data in line with the law;
2. Public sector (i.e. government authorities, public administration bodies, local self-governance and local administration bodies, companies and other legal entities and entrepreneurs which perform public authorisations) is allowed to process biometric data in relation to entry to the business or official premises and presence of employees at work, if such measures are prescribed by the law;
3. The aforementioned measures can be regulated if necessary for the purpose of security of people or property or for the purpose of protecting secret data or business secrets, provided that such objective cannot be achieved in a different manner, or for the purpose of executing obligations from international agreements and determining identity of persons who cross the territorial boundary.

On the other hand, unlike biometric data, the Current Data Protection Law does not recognise genetic data and establishes no rules regarding their processing.

Nevertheless, as already mentioned above, it does establish rules on video-surveillance. It governs it as one of the so-called special cases of data processing. Specifically, there are four situations explicitly prescribed by the respective law as the cases when, subject to fulfilment of the prescribed conditions, video-surveillance is allowed, as follows: (1) video-surveillance of access to official or business premises, (2) video-surveillance in official or business premises, (3) video-surveillance of entrance to/exit from residential buildings and joint premises, and (4) video-surveillance of public surfaces. In any case, there should be a visible notification of video-surveillance so that the individuals approaching the respective premises/buildings would be aware of its existence and would be able to decide not to enter the particular premises/buildings if they do not want to be subject to the respective surveillance.

Coming back to the special categories of personal data which are governed by the Current Data Protection Law, their processing is prohibited except for a few exceptional cases explicitly envisaged by the Current Data Protection Law ("**Exceptional Cases**").

The Exceptional Cases are the following:

1. If a data subject has given explicit consent to the processing of such data;
2. Processing is necessary for the purpose of employment in line with the employment law, whereas adequate security measures should be determined;
3. Processing is necessary for the detection, prevention and diagnosis of diseases and treatment of individuals, as well as for managing healthcare services, if such data is processed by a healthcare professional or other person who has a confidentiality obligation;
4. Processing is necessary for the protection of life or other vital interests of the data subject or of another person, if such person is not capable of providing consent personally, as well as in other cases prescribed by the law;
5. If a data subject has manifestly made personal data available to public or their processing is necessary for pursuing or protecting that person's legal interests before a court or other authorities;
6. If the processing is performed as part of legitimate activities or a non-profit organisation – of an association or other non-profit organisation with political, philosophical, religious or trade union objectives, under condition that the processed data relate solely to the members of the respective organisation or to the persons who have regular contact with the same in relation to the purpose of its activities and under condition that the respective data are not published without the data subject's consent.

Accordingly, no processing of special categories of personal data is allowed if it does not "fit in" one of the Exceptional Cases. From that point of view, the Current Data Protection Law is aligned with the GDPR, however it should be noted that the above list of the Exceptional Cases envisaged by the Current Data Protection Law does not fully correspond to the respective list envisaged by the GDPR.

For example, one of the Exceptional Cases from the GDPR List (Article 9) which is not included in the above list is the case of processing necessary for reasons of substantial public interest or processing necessary for archiving purposes in public interest, scientific or historical research purposes or statistical purposes.

Further, it is worth mentioning that, under the Current Data Protection Law, any processing of the respective data, when allowed, is subject to various additional obligations (e.g. they should be specially designated as such and protected against any unauthorised access). Further details regarding such additional obligations are envisaged by the rulebook which governs special categories of personal data, as identified and elaborated under Chapter IV, Section 2, item 10.

Considering all the above, it can be concluded that significant similarities do exist between the regime of special categories of personal data under the Current Data Protection Law

and the respective regime envisaged by the GDPR. However, certain differences are evident as well. Accordingly, there is no full alignment of the Current Data Protection Law with the GDPR when it comes to special categories of personal data.

5. RIGHTS OF DATA SUBJECTS

Although certainly not as systematic and detailed as the GDPR (Chapter III – Rights of the data subject), the Current Data Protection Law does provide for some data processing related rights of data subjects.

These are the following rights:

1. Right to be informed on a particular processing which involves his/her personal data;
2. Right to rectification (i.e. if a data controller establishes that processed data are incomplete or incorrect, it is obliged to supplement or amend them, the same as if it receives the respective request from the data subject);
3. Right to deletion (i.e. if a particular data processing is not compliant with the law, a data controller is obliged to delete the processed data upon request of the data subject);
4. Right to restriction of the data processing (e.g. if the processed data accuracy is contested by the data subject);
5. Right to withdraw consent (if consent is a legal ground for a particular data processing);
6. Right to object to the data processing (such as if the processing is to be performed for direct marketing purposes), and
7. Right not to be subject to a decision based solely on automated processing (i.e. unless exceptionally, evaluation of the data subject's personal characteristics and capacities, such as, for example his/her results at work, reliability and behaviour, cannot be based solely on automated processing, when deciding on that person's rights, obligations and interests).

The Current Data Protection Law further prescribes that data subjects are entitled to be informed whether their personal data is processed within 15 days from the day when they file such request. The same term is prescribed as the period within which a data controller is obliged to pass a decision on the data subject's request for data rectification or deletion. It is also prescribed that the data subject rights may be limited due to some specific circumstances (such as, for example, for the reasons of national and public security, or for the purpose of preventing criminal offences), but, in any case, only to the extent necessary for achieving the purpose for which a particular restriction is established.

Further, if a data controller would not respond to a data subject's request or if it would refuse to act upon the same, the data subject would be entitled to file a complaint with the respective data controller or to submit a right protection request to the Agency. Such request can also be filed with the Agency by any person who considers that his/her rights envisaged by the Current Data Protection Law are infringed, whereas the Agency should decide on such request within 60 days from the day when a particular request was filed. The Agency's decision cannot be appealed, but administrative dispute can be initiated against it before the competent court.

Considering all the above, it can be concluded that the current regime of the data subjects' rights is not fully aligned with the GDPR (for example, data portability right is not provided at all) and its further improvement is yet to follow, but it does not contravene the GDPR data processing principles either.

6. REGISTRATION AND RECORDS OF DATA PROCESSING ACTIVITIES

Unlike the GDPR which prescribes the obligation of data controllers/processors to keep records of their data processing activities (i.e. of their databases) (Article 30), but not the obligation of the respective database registration with the competent data protection authority, the Current Data Protection Law governs both the obligation of data controllers to keep records of their data processing activities (i.e. of their databases containing personal data) and obligation to register their databases with the Agency.

Specifically, if they intend to establish an automated database, they are obliged either to notify the Agency of its intended establishment or to obtain its prior approval for such establishment, depending on the particular processing characteristics (i.e. whether it involves a particular risk to rights and freedoms of data subjects). Accordingly, the Agency keeps the registry (available to public) of the respective databases. Exceptionally, information on the respective databases (i.e. on the processing covered by the same) is nor entered in the registry if such exception is required by the interests of defence, national and public security or protection of life and health of people, upon previously obtained opinion of the competent authority.

It should also be mentioned that a prerequisite which needs to be fulfilled for the respective database registration with the Agency is the initial registration of the data controller as such.

As already mentioned at the beginning of this item 6, the Current Data Protection Law is not aligned with the GDPR when it comes to the registration of data processing activities. This is due to the fact that, unlike the Current Data Protection Law, the GDPR does not govern either the obligation of registering databases containing personal data with the competent data protection authority or the obligation of prior registration with the Agency of the data controllers themselves. The GDPR only governs the obligation of data controllers/processors to keep records of their data processing activities (i.e. of their databases), whereas the types of information which should be included in these records is explicitly prescribed (e.g. types of the processed data, categories of the data recipients, purpose(s) of the data processing, information on the transfer of processed data out of economy, etc.).

For the sake of completeness, and also considering that Montenegro should get its fully aligned GDPR law in the (relatively) near future, it is worth mentioning that the GDPR also governs that the above-described obligation of keeping data records shall exist only if data controllers/processors have at least 250 employees or, regardless of their employee number, if the processing is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data or personal data relating to criminal convictions and offences.

7. DATA BREACH RELATED NOTIFICATION AND DATA PROTECTION IMPACT ASSESSMENT

Both the obligations regarding data breach related notifications and data protection impact assessment are novelties introduced by the GDPR (Articles 33 – 36). From the perspective of these two novelties, the Current Data Protection Law is not aligned with the GDPR.

In other words, the Current Data Protection Law does not recognise either the institute of data breach related notification or the institute of data protection impact assessment.

Accordingly, the respective institutes are currently inapplicable in Montenegro, at least from the perspective of general data protection rules. This means that the data breach notification institute is recognised by certain sectoral laws currently applicable in Montenegro, such is, for example, the Law on Electronic Communications ("**EC Law**").

The EC Law governs that electronic communication activities are based on, amongst other, ensuring protection of personal data and privacy and obliges operators to notify, without undue delay, the Montenegrin Agency for Electronic Communications and Postal Services and the Agency of any breach of personal data or privacy of the data subjects.

It is further prescribed that this notification should particularly contain a description of the consequences of respective breach, as well as the measures proposed or undertaken for the purpose of eliminating the cause of the breach.

In addition to notifying the relevant authorities, as identified above, the EC Law obliges the operator to notify the data subjects (i.e. users of the respective telecommunication services) if a particular breach may influence detrimentally the user's personal data or privacy. This notification has to contain description of the particular breach along with referencing the user to the operator's authorised person from whom additional information may be obtained, as well as the proposal of measures for mitigating negative consequences of the respective breach. Additionally, operators are obliged to keep records of personal data breaches which should contain information on the causes of respective breach, consequences of the breach and implemented safeguards.

Non-compliance with the above-identified obligations imposed by the EC Law may lead to liability for misdemeanour and prescribed sanctions are fines in the amount of up to EUR 30,000 (for a legal entity) and up to EUR 3,000 (for the legal entity's responsible person). Additionally, if any material benefit would have been gained by committing the respective misdemeanour, such benefit would be seized as well.

Coming back to the above-described obligations governed by the GDPR – the data breach related notification and data protection impact assessment, the Current Data Protection Law is not aligned with the GDPR at all, considering that none of the respective obligations is recognised by the respective law.

8. DATA TRANSFER

When it comes to the data transfer regime governed by the Current Data Protection Law, it could be said that there are two main components of the respective regime.

The first one is that personal data may be transferred out of Montenegro if an adequate level of personal data protection exists and subject to the Agency's approval, whereas the Agency issues such approval only if it establishes that adequate measures for the protection of personal data are undertaken (considering, for example, the processed data's nature, purpose of the respective transfer, statutory rules in force in the economy to which the data is to be transferred, etc.).

The second "component" of the respective data transfer regime includes the explicitly prescribed cases when a data transfer out of Montenegro can be performed without any approval of the Agency. These are the following cases:

1. Data subject provided his/her prior consent to the particular transfer and was made aware of possible consequences of such transfer;
2. Data transfer is prescribed by a particular law or an international agreement which obliges Montenegro;
3. Data transfer is needed for performance of an agreement between a legal entity or natural person and data controller or for fulfilling pre-contractual obligations;
4. Data transfer is needed for saving life of the data subject or when the transfer is in the data subject's interest;
5. Data transfer is made from registries or records which, in line with a law or other regulation, are publicly available;
6. Data is transferred to the economies which are members of the European Union and European Economic Area or to any economy which is on the EU adequacy list;
7. Data transfer is necessary for fulfilling a public interest or for fulfilling or protecting the data subject's legal interests;
8. Data controller enters into an agreement with a data processor from a non-EU economy, whereas such agreement includes adequate contractual obligations accepted by the member states of the European Union;
9. Data transfer is needed for conclusion or performance of an agreement between a data controller and a natural person or a legal entity, when such agreement is in the interest of the data subject.

Considering the above, it can be concluded that, although full alignment with the GDPR is certainly needed, the Current Data Protection Law already provides relatively broad scope of possibilities for performing legitimate transfer of personal data out of Montenegro.

From the cross-border/boundary data protection perspective, it should also be noted that, considering that all the jurisdictions in the region have already adopted GDPR aligned laws (such as Serbia or North Macedonia) or should adopt them relatively soon (such as Albania or Bosnia and Herzegovina), we do not perceive any particular cross border/boundary data protection issues which should be regarded as unsolvable or burdensome in the region.

For the avoidance of any doubt, the precondition which should be fulfilled for the realization of the above cross-border/boundary data protection "scenario" in the region, is that the local data protection laws (already aligned with the GDPR or about to become aligned) should be duly, consistently and continuously applied and implemented, the same as any other regulations adopted on the basis of the respective laws, by the data protection and other relevant authorities in each of the jurisdictions. Amongst other, this means that local authorities would not develop/support any practice/requirements which would be harsher for data controllers/processors in comparison to the requirements introduced by the GDPR (and, thus, by the local data protection legislation as well). Otherwise, the environment of legal uncertainty may be created and such environment would certainly not be the ground for further development on either local or, particularly, regional level.

9. PENAL POLICY

The penal policy prescribed by the Current Data Protection Law is significantly, although not surprisingly, milder than the penal policy introduced by the GDPR.

This is due to the fact that, unlike very stringent penal policy and extremely high fines introduced by the GDPR (i.e. fines in the amount of up to EUR 20,000,000 or 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher), the Current Data Protection Law prescribes offence liability for breaching the law, whereas the highest amounts of the fines for such breaches are EUR 20,000 for a legal entity and EUR 2,000 for a legal entity's representative or a natural person, per offence.

Although offence liability under some other laws in force in Montenegro (for example, the Consumer Protection Law, Law on Electronic Communications, Corruption Prevention Law, etc.) includes, besides fines, certain additional sanctions/protective measures (e.g. prohibition to perform certain business activities/duties within certain period of time), such additional sanctions/measures are not envisaged by the provisions of the Current Data Protection Law.

Additionally, criminal liability is also prescribed by the relevant Montenegrin legislation. Specifically, the Montenegrin Criminal Code, available on the website of the Montenegrin Ministry of Justice https://mpa.gov.me/biblioteka/zakoni?alphabet=lat, introduces a

criminal offence of *Unauthorised collection and use of personal data* (Article 176.) which is part of the category of criminal offences jointly referred to as *Criminal offences against freedoms and rights of people and citizens*. The prescribed sanction is a fine (in the amount to be determined by the court) or imprisonment up to 3 years. However, in general, considering the existing practice, criminal liability remains to be a theoretical possibility.

10. RELEVANT SECONDARY LEGISLATION

In addition to the Current Data Protection Law, a variety of subordinate legislation (such a rulebooks and rules) is also part of the Montenegrin regulatory framework governing data protection and privacy.

As it is expected that Montenegro will get its new GDPR aligned data protection law in the (relatively) near future, the new subordinate legislation is also expected to be adopted. Nevertheless, for the sake of completeness and providing the broader picture of the entire regulatory framework, the overview of the current secondary legislation (i.e. of the main areas it governs) follows below.

I. **Special categories of personal data** – The definition and rules on the processing of the respective data (general prohibition subject to certain exceptions when the processing is allowed) are governed by the Current Data Protection Law, whereas the Rulebook on the Manner of Marking and Protection of Special Categories of Personal Data (2011) (available on Agency website http://www.azlp.me/me/propisi) prescribes further rules on their processing (i.e. on their marking and protection) including also identification of specific measures (technical, organisational and human resources) which should ensure their protection. The Montenegrin Ministry of Interior has passed this Rulebook.

   Firstly, it is prescribed that all data controllers, including both public and private sector, are obliged, when processing any personal data which belongs to special categories of personal data, to mark them by putting the marking "Special category of personal data".

   Secondly, every data controller is obliged to adopt a plan of protection of special categories of personal data ("**Protection Plan**") and to ensure implementation of organisational, technical and human resources measures for the protection of the respective data.

   The Protection Plan should be made in a written form, should be updated regularly and should be available to the Agency at all times. It contains the processed types of special categories of personal data and list of undertaken technical and organisational measures, whereas the respective measures should ensure the following:

   1. Only authorised persons are entitled to process this data;
   2. The processed data are to remain unchanged, complete and accurate in the course of their processing;
   3. They should be available to the data controller all the time and their correct processing should be enabled;
   4. The processed data origin can be established at any moment and it can also be established which person(s) processed the respective data, as well as which data, when and how;
   5. The complete process of the respective data processing is duly recorded.

   It is further prescribed that the respective measures should ensure that the work with special categories of personal data is conducted solely in the course of the data controller's regular working hours, and that the respective data are encrypted during their transmission through telecommunication systems.

   The types of technical human resources and organisational measures are explicitly identified as well.

   Specifically, it is envisaged that the technical measures are to disable unauthorised access and processing of the respective data and they include control of access to premises and equipment for data processing, protection from destroying and damaging of the processed data, as well as other measures which are suitable considering the nature and type of the processed data.

   On the other hand, organisational and human resources measures include the following: training of the employees involved in the processing of special categories of personal data, measures of physical protection of the premises and of equipment used for processing of personal data, preventing any unauthorised copying, multiplication, transcription and destruction of the respective data, as well as any other measures which are suitable considering the nature and type of the processed data.

II. **Records of data processing activities** – Further details on the manner of keeping such records, as envisaged by the Current Data Protection Law, as well as their form, are prescribed by the Rulebook on the Form and Manner of Keeping Record of Personal Databases (2010) (available on the Agency website http://www.azlp.me/me/propisi).

   Specifically, this Rulebook, which was passed by the Montenegrin Government, the same as the Rulebook under point i above, governs the content of the respective records in detail.

   The following information on data processing should be included in the records of the respective data processing activities:

   1. Identification of the data controller;
   2. Legal grounds for the respective processing;
   3. Data processing purpose;
   4. Types of the processed data;
   5. Manner of the processed data's collection;
   6. Manner of keeping the processed data and their retention term;
   7. Information on the processed data's use;
   8. Information on their transfer out of Montenegro, if any;
   9. Information on the internal rules of the data controller governing the processing and protection of the respective data, as well as the security measures undertaken.

      The exact form in which these records should be kept, in a hard copy or electronic format, is also explicitly prescribed and represents an integral part of the respective Rulebook.

III. **Operation of the Agency** – Numerous bylaws (such as the Rules on the Work of the Agency for Protection of Personal Data and Free Access to Information (2013) and Rulebook on the Business of the Agency for Protection of Personal Data and Free Access to Information (2017)), which are available on Agency website http://www.azlp.me/me/propisi, govern the variety of issues relating to the work and operation of the Agency, such as its internal organisation, its employees and bodies, public procurements, relationship with/obligations towards other government authorities, budget, etc.

   Considering that the respective regulations contain rules regarding the Agency's internal governance (and not the rules on processing of personal data), these rules are

not subject to our further analysis, nevertheless some of them are included in Section 3 below considering that it contains information on the Agency itself in the context of its competence and challenges in its work;

IV. **Surveillance by the Agency** – The Agency competences, including its surveillance authorities, are governed by the Current Data Protection Law. Detailed rules on the manner in which the Agency monitors the implementation of the respective law are envisaged by the Rulebook on the Manner of Conducting Surveillance in the Field of Personal Data Protection (2018), which is available on Agency website http://www.azlp.me/me/propisi)

This Rulebook, which was passed by the Agency in 2018, governs how and why and by whom in the Agency the respective surveillance is conducted. It is emphasised that the principal purpose of the surveillance is prevention for the purpose of encouraging responsible and legitimate behaviour of entities which process personal data (regardless of whether they are in public or private sector).

The surveillance is performed either ex *officio* or upon written request of a person who considers that his/her rights are infringed. Depending on the circumstances of each particular case, authorised persons in the Agency ("**Controllers**" in the meaning of inspectors) conduct the surveillance either from their office or in the premises of a controlled entity directly. The inspection is preformed from the office in the case when the factual background can be established without any doubt on the basis of publicly available data (such as through media, Internet, etc.).

Depending on the reasoning behind/grounds for conducting the surveillance, it can be regular, extraordinary or a control one. The regular surveillance is performed in line with the annual work plan of the relevant department. Surveillance is usually announced to the inspected entity at least 3 days in advance, in writing, unless the inspection's purpose would be endangered by such prior announcement.

The Controllers have a broad range of authorisations when performing inspection including the following:

1. To enter all premises in which personal data is processed;
2. To inspect all premises, documents and records in which personal data may be contained, as well as all other records, contracts and other business documentation;
3. To determine identity of the controlled entity and of other persons;
4. To take statements from a responsible person and other persons;
5. To take documents needed for establishing factual background;
6. To order taking appropriate measures and activities;
7. To temporarily seize documentation and other items necessary for establishing a factual background;
8. To initiate prohibition of performance of particular activities;
9. To undertake other prescribed measures;
10. If they determine that personal data is processed contrary to the law, they ask for termination of such processing and order other measures which the controlled entity is obliged to perform within designated period of time (such period should not be longer than 15 days except when, due to complexity of a particular matter, it can be up to 60 days).

    The Controllers are obliged to make minutes of each particular inspection (on the form prescribed by the aforementioned Rulebook) and to describe the factual situation determined by such inspection.

They are employees of the Agency and are obliged to keep confidentiality of the information they find when performing inspections.

3. COMPETENCE OF AND CHALLENGES IN THE WORK OF THE AGENCY

The public authority with the competence in the field of data protection is the Agency for Personal Data Protection and Free Access to Information (in Montenegrin, *Agencija za zaštitu ličnih podataka i slobodan pristup informacijama*).

The Agency is an autonomous public authority established by the Current Data Protection Law more than 10 years ago. It is independent in its work. It submits regular annual reports on the state of play in the field of data protection ("**Annual Report**") to the Parliament of Montenegro. The Annual Report should be provided by 31 March of current year for the previous year.

In addition to the Annual Report, the Agency also submits to the Parliament a special report on the state of play in the field of data protection if the Parliament requires that or if the Agency estimates that there are special reasons for submitting such report.

The Agency's bodies are the Council and Director. Upon the Director's proposal, the Council appoints the Agency Secretary and also establishes the annual work plan of the Agency ("**Work Plan**") which, amongst other, contains information on the resources needed for one-year period covered by the respective annual plan.

The Agency has its expert team which is coordinated by the Secretary. The following organisational units are integral parts of the Agency:

1. Department for Monitoring of Personal Data Protection;
2. Department for Personal Data Protection Matters and Complaints;
3. Department for Access to Information;
4. Department for Registry and Information System;
5. Department for Legal, General and Accounting Affairs.

When it comes to the Agency's financing, the principal source of funding is the government budget (other sources are also allowed in line with the law). Information on the exact purposes for which the budget resources provided to the Agency are spent (e.g. salaries of employees, travel expenses, expenses for office equipment and materials, etc.) and on the exact amount of each of such spending is published on the Agency's website (according to the latest published data – 2018 Annual Report, the total amount of Agency budget for the respective year was EUR 617.323,69).

In this regard, it is explicitly envisaged by the 2020 Work Plan that the performance of the Agency's activities envisaged is either (1) covered/is to be covered by regular budget resources or (2) does not require any particular resources or (3) requires the exact amount of money on the annual level (such as the amount of EUR 2,000 for activities such as the education of general public in the field of data protection, promotion of the Agency's work, preparation of projects/participation in joint projects for the purpose of further development of data protection) or (4) should be covered by the resources from EU funds (no further identification of such funds in envisaged by the respective Work Plan).

Also, according to the list of employees for 2020 published on the Agency's website, the Agency has a total number of 31 employees out of which only four are the so-called controllers (i.e. inspectors), thus only four of them are engaged in inspection supervision of the Current Data Protection Law, as elaborated above in Section 2 (item 10, point iv.) of this Chapter.

Under presumption that the respective figures are accurate, it can be concluded that the lack/insufficiency of staff, such as in the field of inspection supervision, is indeed a significant issue in the current functioning of the Agency.

The Agency's competences are set in detail by the Current Data Protection Law. These are the following:

1. Monitoring implementation of the respective law;
2. Acting upon data protection requests filed with the Agency;
3. Issuing opinions regarding application of the respective law;
4. Approving establishment of databases containing personal data;
5. Issuing opinions if there is a doubt whether a particular group of personal data should be regarded as a database containing personal data;
6. Monitoring implementation of organisational and technical measures for the protection of personal data and proposing improvements of such measures;
7. Providing proposals and recommendations for improving protection of personal data;
8. Issuing opinions on whether a particular manner of processing threatens the rights and freedoms of individuals;
9. Cooperating with competent data protection authorities in other economies;
10. Proposing assessment of constitutionality and legality of laws or other regulations and general acts by which processing of personal data is governed;
11. Performing other activities in line with the relevant laws.

The Agency is not authorised to submit proposals of new laws to the Parliament. It is, therefore, of utmost importance, as regards the laws governing/relevant for the processing of personal data, that active cooperation exists between the Agency and relevant Ministries within the Government, as that is the proper way for ensuring that the best laws are submitted to and adopted by the Parliament.

The Agency's cooperation with other government authorities is of substantial importance as well since it is necessary for adequate implementation and further improvement of the local data protection legislation. This is due to the fact that processing of personal data is an integral part of day-to-day operations of numerous business entities and institutions, as well as of both public and private sector, such as, for example, in the field of telecommunications, healthcare, education, banking, insurance and many other. This further means that applicable sectoral laws should be fully harmonised with the relevant data protection requirements.

Coming back to the Agency's competences, the Agency has two types of powers for exercising its authority and duties within its competence, as follows:

1. Powers relating to its capacity of a second-instance authority responsible for protecting the right to data protection in appeal proceedings (i.e. based on the data protection requests filed with the Agency) ("**Appeal Related Powers**") and
2. Powers relating to its capacity of a supervisory authority responsible for enforcing the Current Data Protection Law ("**Supervisory Powers**").

When it comes to the Agency's Appeal Related Powers, it decides on filed data protection requests within 60 days from the day of their filing. Depending on whether the Agency finds a data protection request grounded, it may reject it (if ungrounded) or order the data controller to act upon the request within a specified period of time (if grounded). In any case, no appeal can be filed against a decision passed by the Agency, but an administrative dispute can be initiated against such decision (or if the Agency does not pass a decision within the statutory term) before the competent court.

When it comes to the Agency's Supervisory Powers, the Agency is entitled, amongst other, to order certain corrective measures to data controllers/processors (e.g. to temporarily ban the data processing non-compliant with the law, order removal of the existing irregularities within certain period of time, etc.), as well as to file a request for initiating offence proceedings against them before the competent court.

The support (other than the aforementioned government budget allocation) the Agency (potentially) receives for the purpose of further development of data protection policies and practice in Montenegro is very important as regards its work and organisation.

Based on the information publicly available on the Agency's website, the Agency participated in **a few Twinning/Twinning Light projects funded by the EU**, but we have found (at least not on the website of the Agency) no information on other international projects in which the Agency may have been (or is currently) involved.

It was also confirmed, through a written (e-mail) correspondence with the competent authorities (with the representative of the Montenegrin Ministry of Internal Affairs), that there are no ongoing data protection related projects at the moment. In relation to the respective e-mail correspondence (exchanged in September 2020), it should be mentioned that it was explicitly confirmed in a phone correspondence with the representative of the Agency (which took place in October 2020) that all the information from the aforementioned e-mail correspondence (thus, aforementioned information on the respective (lack of) international projects) was prepared jointly with the Agency.

On the other hand, it is publicly announced on the Agency's website www.azlp.me that it has entered into Memorandums of Cooperation with the data protection authorities from Serbia, Republic of North Macedonia and Albania. These agreements were entered into in 2011 (with Albania and Republic of North Macedonia) and in 2017 (with Serbia). These are the only documents published on the website of the Agency which govern its international cooperation (http://www.azlp.me/me/medjunarodna-saradnja). Therefore, we presume that these are the only agreements of that kind which the Agency has entered into.

Considering all the above-stated information on the operation and competences of the Agency, as well as the fact that the Current Data Protection Law is not the GDPR fully aligned law, the main challenge the Agency faces is the adoption of the Data Protection Law which is fully harmonised with the GDPR.

The respective adoption shall further lead to the need for achieving harmonisation of other relevant Montenegrin legislation with such new GDPR aligned law. Considering that the achievement of the respective objectives requires significant resources, more staff and budget should be allocated to the Agency. Obtaining such additional resources will be a challenge of its own. The same is true of the objective of raising public awareness and advocacy of the data protection importance considering that the current level of such awareness is low in Montenegro. This should be kept in mind and further worked on, considering that no significant improvement of data protection environment is possible without improvement of public awareness of the importance of adequate protection of personal data.

4. CHALLENGES IN THE IMPLEMENTATION OF THE CURRENT DATA PROTECTION LAW IN PRIVATE AND PUBLIC SECTOR

The current challenges in the field of data protection law in Montenegro include both the challenges faced by the Agency, as described above in Section 3 of this Chapter IV, and

challenges faced by local entities involved in data processing activities in the capacity of either data controllers or data processors ("**Local Processing Entities**").

When it comes to the Agency, the main challenges are, as already mentioned above, the following:

1. Full alignment of the local data protection legislation with the GDPR, and
2. Understaffed institutional capacity of the Agency.

When it comes to the full alignment of the local legislation with the GDPR, this is certainly the challenge of crucial importance. Montenegro has not adopted its new GDPR aligned law yet, but such adoption is expected to happen in (relatively) near future – by the end of 2020. It is questionable, in particular considering the ongoing Covid-19 pandemic, whether the respective objective will be achieved so soon, but, regardless of the fact whether it shall indeed happen by the end of this year or in the course of the following one, the actual implementation of the rules and requirements imposed by such new law shall be a big challenge. The same goes for harmonisation of other relevant legislation and sectoral laws in Montenegro with such new GDPR fully aligned law.

When it comes to the Agency's institutional capacity, it has total of 31 employees. Considering that the Agency has dual competence (competence for personal data protection and competence for free access to information of public importance) this number seems insufficient for covering all the activities the Agency is to undertake. This lack of human resources should be further emphasised as regards the number of Agency's employees engaged in inspection supervision of the Current Data Protection Law – there are only 4 of them. Thus, it does not come as a surprise that the Agency is not as active as it should be and that the current level of enforcement is rather low in Montenegro.

One of the main obstacles identified for further development of data protection law and environment in Montenegro is the mentioned low level of enforcement. In addition, the penal policy introduced by the Current Data Protection Law is rather mild if not symbolic in comparison to the draconian fines imposed by the GDPR.

Finally, low level of public awareness about the importance of personal data protection and poor knowledge of the data processing related rights is a reality in Montenegro. The same goes for awareness and/or knowledge of/resources for fulfilling the obligations which the Local Processing Entities have under the Current Data Protection Law.

In summary, the main challenges in the field of data protection law in Montenegro are currently the following:

1. Low public awareness on data protection importance and of available legal resources;
2. Low level of implementation of the Current Data Protection Law;
3. Low level of enforcement;
4. Mild penal policy.

Once the new data protection law, aligned with the GDPR, enters into force, it will become even more difficult for private and public sector entities to correctly enforce data protection legislation given that proper implementation of new principles, such as accountability, requires them not only to be compliant with the law, but also be able at any time to document and prove their compliance. Besides the principle of accountability, one of the most challenging principles to comply with would be the GDPR's principle by design and default.

This is due to the fact that the implementation of respective principles would require the Local Processing Entities to respect the data protection requirements from the very creation/further development of their IT system as, otherwise, they would not be able to respond to or address the challenges which the new GDPR aligned law imposes (such as, for example, the requirement to ensure exercise of data subject rights and to ensure such exercise is made within the terms envisaged by the law, or requirement to timely prepare and file data breach notifications).

Accordingly, full and adequate implementation of the GDPR aligned law would require significant resources (e.g. for obtaining adequate equipment/software and hiring qualified personnel) for the vast majority of the Local Processing Entities.

The data minimisation principle should also be mentioned. Its application may be challenging in practice, both in private and in public sector, considering that various types of records/registries are kept by the Local Processing Entities and include much personal data, whereas not all of them are absolutely necessary for the achievement of their legitimate processing purposes. Minimising the retention terms whenever possible will be a challenge of its own.

Considering the above circumstances, data controllers and data processors in Montenegro (on which significant obligations are yet to be imposed upon adoption and entry into force of new GDPR aligned law) may ask themselves why to invest resources and efforts in reaching full compliance with the respective law, if there would be, due to very mild penal policy and low level of enforcement, no or at least no significant consequences for their non-compliance.

For the sake of avoiding such scenario – avoiding that the environment of non-compliance would become/remain the "normal" state of affairs which does not lead (and/or is not perceived to lead) to any actual fines, other sanctions or any other relevant consequences regardless of the breaches of the law which may have been committed, the following steps should be undertaken as the priority:

1. Adoption of the new data protection law fully aligned with the GDPR and harmonisation of all related legislation and sectoral laws with the GDPR aligned data protection law, as well as strengthening capacities of the Agency ("**Adoption of the New Law and Further Harmonisation of the Relevant Local Legislation**");
2. Raising public awareness on the data protection importance (in particular when it comes to the rights data subjects have under the Current Data Protection Law, but in general as well), whereas this should further lead to the more significant reputational risk for the Local Processing Entities ("**Raising Public Awareness on Data Protection Importance**");
3. Regular and continuous education and training of individuals involved in the processing of personal data both in the public and private sector ("**Data Processing Related Education and Training**");
4. Intensifying inspection supervision of the Current Data Protection Law implementation (to the extent possible considering the existing staff restraints faced by the Agency) ("**Intensification of Inspection Supervision**");
5. Commencing and conducting offence proceedings before the competent courts against all data controllers/processors breaching the law ("**Offence Proceedings**");
6. Emphasising possible applicability of the GDPR, due to its extraterritorial effect, to the Local Processing Entities ("**Extraterritorial Effect of the GDPR**").

If we would have to identify which of the above-identified steps is the crucial one, this would always be, besides the obvious one (i.e. adoption of the new GDPR aligned law, and further harmonisation of the relevant local legislation with such new law, along with strengthening the Agency's capacities), EDUCATION as it is the starting point for any development of data protection law and environment.

If individuals as the data subjects (regardless whether they are consumers, employees or simply citizens in their everyday life) would be aware of the importance which adequate protection of personal data has for their lives – if they would be aware of the risks (e.g. identity stealing risk) which unauthorised processing/misuse of personal data may expose them to, and if they would have sufficient knowledge of the statutory rights which belong to them as data subjects, they would certainly boost the existing data protection environment.

By reacting to potential non-compliant activities of local data controllers/processors adequately, regularly and timely, they would exert pressure to the respective entities to be more careful and more compliant with the data protection law when it comes to their processing activities (in particular from the perspective of the types and scope of the processed data). Otherwise, they could be exposed to the inspections by the Agency (and, consequently, other state authorities/competent inspectors), court proceedings, offence and other legal liability, as well as significant reputational risk (which is often more important than material damage/fines which they may be obliged to remunerate/pay).

Besides education, proper ENFORCEMENT is always crucial. Regardless of their level of knowledge and awareness data subjects need to be supported by the entire system - by competent authorities, as only these can ensure that breaches of any law (thus, of the Data Protection Law as well) are sanctioned fully and adequately.

5. CRUCIAL STEPS FOR OVERCOMING THE EXISTING CHALLENGES

For the sake of creating a compliant environment in respect of the existing and future data protection legislation, the list of steps of crucial importance, along with the description of each of them, follows below.

I. **Adoption of the New Law and Further Harmonisation of the Relevant Local Legislation**

Considering that, as already noted throughout this report, no GDPR aligned law has been adopted yet in Montenegro, the adoption and further implementation of such data protection law should be regarded as top priority.

In this respect, as already mentioned in the introductory part of this report, it is expected that Montenegro would get its GDPR aligned law by the end of this year. It is questionable whether such timeframe is feasible at this moment, particularly considering still ongoing Covid-19 pandemic, but regardless whether the new Montenegrin GDPR aligned law would indeed be adopted by the end of 2020 or later on, its adoption would certainly lead to the need for harmonising all the relevant local legislation and sectoral laws with the requirements envisaged by the respective GDPR aligned law.

Considering that the Agency, as the competent data protection authority, should have the leading role in such process, its current capacities (such as in the terms of its staff) should be strengthened. For the sake of illustrating such need, it should be mentioned that, based on the information published on its website www.azlp.me, the Agency has total of 4 employees engaged in inspection supervision of the Current Data Protection Law. It seems that such a number should at least be doubled. Otherwise, it is indeed unrealistic to expect any significant improvements of the current low level of both the implementation of the data protection law and of enforcement in the field of data protection.

II. **Raising Public Awareness on Data Protection Importance**

Low level of public awareness, when it comes to the importance of data protection and of adequate data processing activities, is one of the main challenges in the field of data protection law in Montenegro at the moment, as already stated in Section 4 of this Chapter IV.

Consequently, public awareness should be raised and education of the public should be carried out consistently and persistently. Education of the public is the starting point and one of crucial mechanisms for further development of data protection law and environment.

It can be carried out, amongst other, by media campaigns, as well as by data protection training which could start even in schools. For this purpose, the Agency could cooperate with the Montenegrin Ministry of Education.

As a general remark, regular communication and cooperation between relevant authorities is of principal importance in practice, as it enables sharing knowledge and discussing current issues and mechanisms for addressing them jointly to the extent feasible. Lack of such communication and cooperation would certainly represent a burden (if not even a "show stopper", at least to a certain extent) for overall development of data protection law in the economy and for full implementation of the GDPR based processing principles and rules expected to be envisaged by the new Montenegrin GDPR aligned law.

Coming back to the objective of raising public awareness on data protection importance, it should be mentioned that the Agency should be very proactive, open and transparent in its activities. Its representatives should be much more present in media, conduct/participate in media campaigns and organise data protection training.

Furthermore, the Agency should also publish much more materials on its website. However, these should not be solely materials of formal nature such as annual reports, work plans, applicable laws and other regulations, but should include interactive presentations, handbooks, practical guidance, checklists and other similar materials, which would be simple, informative and easily understandable by the broadest possible range of data subjects and data controllers/processors in Montenegro and which, as such, would serve to "popularise" the data protection law and acceptance of its importance (as no acceptance can happen without prior understanding of the matters which should be accepted).

Publication of the most relevant information and developments should also be made through social networking platforms, as such platforms are widely used by the general public and communications made through them is expected to reach many concerned individuals.

Additionally, the tool which should be implemented to significantly help the process of raising awareness about data protection is a platform for questions and answers. This platform should be available to everyone to submit a question to the Agency, which would then be responded and saved on the platform where any interested person could access and search through the data protection questions which are most frequently asked (FAQ).

Anyhow, overall transparency and proactive approach of the Agency are of crucial importance not only for raising the level of public awareness and further education of the public, but also for strengthening trust of the public in the Agency itself.

It may also be useful to conduct a study on the level of data protection awareness of the general public. This would offer a clear overview of the current situation, according to which the necessary steps for increasing awareness can be tailored.

All the above is very important because data subjects would be able, only if educated properly, to (1) understand the importance of adequate data protection and seriousness of the risks (e.g. identity stealing risk) to which they may be exposed if their data would be processed contrary to the relevant legal requirements, and to (2) react adequately and timely should any breach of the data protection law occur (e.g. by filing a complaint with the Agency or damage remuneration lawsuit with the competent court). They should also be aware of their rights in respect to the Local Processing Entities which may process their data, because, without adequate knowledge of such rights, they would not be able/not know how and when to use them.

Their knowledge and reactions in the cases when they consider that some illegitimate activities are undertaken would further influence the Local Processing Entities to be more careful and to act in compliance with the data protection law. Otherwise, they could be exposed to the inspections by the Agency (and, consequently, other authorities/competent inspectors), court proceedings, offence and other legal liability, as well as significant reputational risk (which is often more important than material damage/fines which they may be obliged to remunerate/pay).

III. **Data Processing Related Education and Training**

The Local Processing Entities would also to provide regular and continuous education and training to their own employees. This is equally applicable regardless of the fact whether the Local Processing Entities are part of private or public sector, thus equally applicable to government authorities/institutions as well, particularly if they are involved in the processing of special categories of personal data such as health related data.

It is also advisable, considering that the GDPR alignment is inevitable, that the Local Processing Entities perform an internal due diligence on their established data protection system and especially: identify all their databases containing personal data and risks associated with their processing, assess their technical and organisational measures and whether they need to be updated/amended/enhanced, review their agreements with engaged data processors, if any, consider organising data protection training for their employees, review the cross-border/boundary transfers of the processed personal data and whether adequate security mechanisms are undertaken in particular when it comes to the economies which are not regarded as the economies with adequate data protection systems, etc. Based on the completed reviews and assessments, they should also prepare an action plan for achieving compliance with the relevant data protection requirements.

Continuous education of Agency staff is very important as well. It is a prerequisite to ensure that the newest developments in the field of data protection law can be followed and that local data protection environment can be improved to the maximum extent possible.

Accordingly, the Agency representatives should take active participation in international events and forums, as well as participate in and take initiatives for joint activities with data protection authorities from other economies, especially from the European Union, but from the Western Balkans region as well. Regular communication and cooperation between all relevant government authorities in Montenegro is also very important.

IV. **Intensification of Inspection Supervision and Offence Proceedings**

These two steps are necessary for further improvement of local data protection practice and environment. Education is certainly the starting point, including both for raising public awareness o data protection importance and for all the entities involved in the local data processing activities, but further measures are needed to ensure better implementation of the data protection law.

Accordingly, the Agency should intensify its inspection supervision activities, considering that the precondition for successful fulfilment of such task and for its regular and consistent performance is prior strengthening of the Agency's current capacities, as already stated in this Section 5 above.

In this respect, the Agency should consider abandoning the current practice of keeping the registry of databases containing personal data as reported to it by the Local Processing Entities. In such a way it would not only "free" its staff of unnecessary administrative burden of keeping such registry (and, thus, make them available for more substantial tasks such as training and actively monitoring the implementation of applicable data protection law), but will also align the Agency's conduct with the relevant GDPR requirements.

Further, offence proceedings should be initiated whenever breaches of the data protection law occur (and are not cured) regardless of whether such breaches are made by the Local Processing Entities in private or public sector.

In other words, the respective proceedings should be initiated without exceptions and should be conducted in a fair and transparent way. To avoid any misunderstanding, this does not exclude the provision of advice and support for achieving compliance with the data protection law, which the Agency should provide to the Local Processing Entities including both data controllers and data processors.

The judges dealing with data protection matters should also be trained and educated on the relevant data protection law as well as on the GDPR and its principles in order to ensure proper and effective judicial protection.

The sanctions/fines envisaged by the Current Data Protection Law are not significant ones (in particular if we compare them with very stringent sanctions imposed by the GDPR), but are nevertheless relevant as establishment of legal liability for breaching the law would certainly harm the entities found liable for breaches, at least from reputational point of view.

V. **Extraterritorial Effect of the GDPR**

When it comes to the expected adoption of the new GDPR aligned law, it should be constantly emphasised not only that such law will impose many strict obligations to the Local Processing Entities (due to which they should already commence preparing themselves for the same), but also that the GDPR itself may be applicable to the Local Processing Entities directly due to its extraterritorial effect.

Considering constant intensification and development of online sales activities (due to the Covid-19 pandemics as well), the possibility of the GDPR application to the Local Processing Entities becomes stronger than ever, in particular if their e-sales channels/on-line shops services are to be offered and available not only to local customers, but to those in the European Union as well.

Further development of an active cooperation with other data protection authorities, especially in the European Union, is advisable. The same goes for the non-EU economies in the region, such as for example, Serbia and North Macedonia, which have already adopted GDPR aligned law and, therefore, have already gained certain experience in this respect.

Finally, special attention should be paid to the Covid-19 pandemic. Considering that Montenegro has already had the draft of its new GDPR aligned law at the time the pandemic began, and that such draft law has not been adopted yet, it is very reasonable to assume that the respective pandemic has already influenced/slowed down the process of adoption of the GDPR aligned law and it subsequent implementation in this economy.

Due to the fast spread and the easy transmission of the virus, it became one of the biggest threats to human life and health, as well as businesses and the economy in 2020. This especially impacted the business operations of large companies employing many employees, as some of them had to cease their work, while others even closed down their companies.

Realising that the Coronavirus will be here for some time and that employers need to adapt to the new situation, they became creative in ensuring that the number of employees infected with the virus is brought to a minimum. In addition to other protective measures which employers undertake, they started using advanced technology, some of which raises data protection concerns, as well as large-scale data processing. Furthermore, revealing personal data of employees which are infected with Covid-19 is also questionable. Data protection concerns caused by the Coronavirus spread in other areas, such as education, media, health system, etc. Even though it is undisputed that the right to human life and

health prevails, it is of crucial importance to keep the data protection rights to the highest level possible.

As it is evident that the Coronavirus will not disappear easily nor very soon, it is highly recommendable that the Agency devotes its attention to achieving a high standard of data protection during the pandemic in Montenegro.

This was not the case so far (as the Agency's activities in relation to the pandemic were not, to say it mildly, at the level at which they should have been) and hence becomes even more important in the forthcoming period.

This means that the Agency should be proactive and that it should, in particular, prepare and publish guidelines on how to deal with the pandemic from a data protection perspective, but also advise public authorities and all data controllers directly, prepare and publish opinions on whether certain technologies and monitoring fulfil the data protection requirements and perform supervisions.

CHAPTER V. REPUBLIC OF NORTH MACEDONIA

1. CURRENT STATUS

The main law governing data protection and privacy in the Republic of North Macedonia is the Law on Protection of Personal Data (Official Gazette of the Republic of North Macedonia, no. 42/20, https://dzlp.mk/sites/default/files/u4/zakon_za_zastita_na_licnite_podatoci.pdf) ("**Current Data Protection Law**"). It superseded the Law on Protection of Personal Data from 2005 ("**Old Data Protection Law**", https://dzlp.mk/sites/default/files/pdf/Zakon_za_zastita_na_licnite_podatoci_2005.pdf) which was applicable as of February 2005; therefore for more than 15 years before the Current Data Protection Law was enacted.

The Old Data Protection Law deficiencies were detected in the course of its application and significant improvements were needed (such as, for example, in the field of data transfer regime or legal grounds for data processing). It was also necessary to align the data protection legislation of the Republic of North Macedonia with the new EU data protection regulation – with the General Data Protection Regulation (GDPR).

The respective alignment is the objective of the adoption of the Current Data Protection Law. The Current Data Protection Law entered into force on 24 February 2020.

The Current Data Protection Law represents a copy of the GDPR in its biggest part. Nevertheless, certain differences do exist, whereas the most obvious one is the stricter regulation in terms of the data transfer rules (as detailed below under Section 2, item 13). Other than this, it should also be noted that the Current Data Protection Law does not envisage any of the recitals introduced by the GDPR and, thus, lacks the explanations as a very important tool for its full understanding and adequate application.

The overview of the most important rules governed by the Current Data Protection Law, compared with the relevant GDPR rules, follows in Section 2 of this Chapter V. The relevant secondary legislation will also be covered by the respective overview.

The authority competent for data protection matters in the Republic of North Macedonia is the Agency for Personal Data Protection of the Republic of North Macedonia ("**Agency**"). The Agency is seated in Skopje and its official website is https://dzlp.mk.

The Agency was established by the Old Data Protection Law (then called the Directorate for Personal Data Protection) as the authority with the exclusive competence in the field of protection of personal data. There was no such authority in the Republic of North Macedonia prior to its establishment. At the moment of the adoption of Current Data Protection Law, it already had more than fifteen years of experience in the field of data protection. Nevertheless, there are still some challenges faced by the Agency which remained even after the adoption of the Current Data Protection Law (such as insufficiency of staff particularly in the field of inspection supervision). Further information on the Agency is provided in Section 3 below.

2. ASSESSMENT OF THE LEVEL OF COMPLIANCE OF THE DATA PROTECTION LAW AND RELEVANT SECONDARY LEGISLATION WITH GDPR

As noted above, the Current Data Protection Law is the copy of the GDPR in its biggest part. Accordingly, the rules prescribed by the respective law are generally aligned with the GDPR,

subject to certain exceptions (e.g. the aforementioned stricter data transfer requirements imposed by the Current Data Protection Law).

This overview contains summary of the most important rules and areas governed by the Current Data Protection Law, as well as the identification of the most important secondary legislation and matters prescribed by such legislation, as follows: (1) general data processing requirements, (2) obligations and responsibilities of data controllers and data processors, (3) joint controllers and controller-processor relationship (4) data protection officers and representatives of foreign entities, (5) special categories of personal data, (6) processing of the data subject's personal identification number, (7) data processing and freedom of speech and information, (8) rights of data subjects, (9) providing personal data to recipients, (10) records of processing activities and registry of databases, (11) data breach related notifications and data protection impact assessment, (12) codes of conduct and certification, (13) data transfer, (14) video surveillance, (15) supervision and data subject's rights to remedy, (16) penal policy, and (17) relevant secondary legislation.

1. GENERAL DATA PROCESSING REQUIREMENTS

Under the Current Data Protection Law, all personal data, regardless of their type, category of data subjects and scope of a particular processing, should be processed in line with certain processing principles explicitly governed by the respective law, as follows:

1. Personal data should be processed for specified, explicit and legitimate purposes;
2. Processing should be done lawfully, fairly and transparently in relation to the data subjects;
3. Processing should be limited to data which is necessary for fulfilment of the processing legitimate purpose(s);
4. Processed data should be accurate and, where necessary, kept up to date;
5. Processed data should not be retained longer than necessary for the purpose(s) for which they are processed;
6. Processing should be performed in a manner that ensures appropriate security of processed data.

The aforementioned requirement of carrying out the data processing lawfully means that, amongst other, it should be based on adequate legal grounds. Such legal ground is either data subject's consent (relating to specified, explicit and legitimate purpose(s)) or one of the remaining grounds explicitly prescribed by the Current Data Protection Law.

These are the following grounds:

1. Necessity of a particular processing for the performance of a contract to which a data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
2. Necessity for compliance with a legal obligation to which the data controller is subject;
3. Necessity for the protection of the vital interests of the data subject or of another natural person;
4. Necessity for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller, and
5. Necessity to serve 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 ("**Statutory Grounds**").

It is evident that each of the Statutory Grounds includes necessity of a particular data processing to achieve a specific legitimate purpose(s).

The legal grounds (i.e. a data subject's consent and the Statutory Grounds) envisaged by the Current Data Protection Law correspond to the data processing legal grounds envisaged by the GDPR. All data processing requirements identified above are also fully aligned with the data processing principles envisaged by the GDPR.

2. OBLIGATIONS AND RESPONSIBILITY OF DATA CONTROLLERS AND DATA PROCESSORS

Data controllers and data processors are obliged to perform data processing in compliance with all the data processing principles described above. There is also the obligation to be able to demonstrate the respective compliance (accountability).

This should be done by implementing appropriate technical, organisational and human resources measures, whereas the nature, scope, context and purposes of the particular processing, as well as the risks of varying likelihood and severity to the rights and freedoms of natural persons, should be taken into consideration. The measures should ensure adequate protection of the processed data including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. The rights of data subjects should be duly protected.

The measures should be reviewed and updated where necessary and, if proportionate in relation to processing activities, they should also include the implementation of appropriate data protection policies.

The same as the GDPR, the Current Data Protection Law does not prescribe the exhaustive list of the respective measures, but solely provides some examples (such as pseudonymisation and encryption) and describes, in general, their purpose and circumstances to be taken into consideration when deciding on their implementation.

Controllers should determine and assess risks (risk management) associated with the personal data, which should cover the following stages:

1. List (overview) of all processes that process personal data;
2. Risk assessment for each process of personal data processing;
3. Implementation and verification of the planned measures; and
4. Conduct periodic security checks.

The controller must conduct periodic security checks, for which an action plan should be prepared, the implementation of which is monitored by the controller's management.

Controllers are obliged to implement an appropriate level of technical and organisational measures which will be proportional to the personal data processing activities. As an exception, controllers which process personal data for less than 10 employees as a single database do not have an obligation to implement technical and organisational measures unless there is a probability that the processing represents a risk for the rights and freedoms of data subjects, if the processing is not occasional or the processing includes special categories of personal data or personal data related to criminal convictions and criminal offenses.

The standard and high level of technical and organisational measures which should be implemented are prescribed by the Rulebook on the Safety of Personal Data Processing. The description of respective measures is provided below.

I. Standard level of technical measures:

1. Authentication of authorised persons - the controller ensures that the login in the information system is done through a single identifier that connects only with one authorised person, keeps records of authorised persons who have authorised access to documents and information system, and establishes procedures for identification and verification of authorised access.
2. Provision of equipment for personal data processing.
3. Segregation of duties and responsibilities - the controller determines the authorised persons who should have access to the information system and provides a clear division of duties and responsibilities according to the need-to-know rule.
4. Control of access to information system - the controller establishes mechanisms to prevent authorised persons from accessing personal data and information and communication equipment with rights other than those for which they are authorised.
5. Providing logs for each access (logs) - in order to ensure identification of any unauthorised (fraudulent) access or misuse of personal data, as well as to determine the origin of these incidents, the controller establishes and keeps records of each access to the information system - logs;
6. Securing portable media - raising awareness of the authorised persons about the specific risks related to the use of portable media and the established procedures for reducing these risks; implementation of measures for backup or synchronisation of mobile workstations in order to protect stored data from loss; encryption measures to protect mobile workstations and mobile storage media; and use of cloud services for backups only after prior analysis of their terms and security guarantees.
7. Internal network protection - restricting Internet access by blocking non-essential services; Wi-Fi network management that includes the use of state of the art encryption methods; Wi-Fi network open for use by persons who are not authorised to be separate from the internal network; in case of remote access, mandatory establishment of VPN connection, with mandatory authentication of the authorised person; ensuring that no administrative panel for content management and system setup is directly accessible via the Internet (remote maintenance is mandatory and performed via VPN); and restricting network traffic by filtering incoming/outgoing traffic on firewall equipment, proxy servers, etc.
8. Securing servers - only authorised persons who have the necessary knowledge may have access to the tools and administrative panels of the servers; application of authorisations with less privileges for persons who are not administrators of the information system; application of a special policy for creating and using passwords for the information system's administrators; install all important updates (updates) for operating systems and applications within a time interval on the basis of risk analysis, but no longer than a week update by setting the system to automatically update (auto update); making backups and their regular verification, and application of the TLS or other protocol that provides encryption and authentication, as a minimum for any data exchange over the Internet and confirmation of its proper application through appropriate tools.
9. Securing the website of the controller - technical measures that will guarantee the correct identity of the site (pharming prevention), as well as the confidentiality of the information it sends or collects through the website.
10. Obligations and responsibilities of the administrator of the information system and of the authorised persons - based on the analysis of risk, a data controller defines the obligations and responsibilities of the administrator and the persons authorised for the use of documents and information and communication equipment, performs mandatory periodic review of the work of the administrator and prepares a report on the performed control.
11. Incident prevention, response and remediation (ensuring continuity) - based on the risk analysis, the controller establishes a plan for continuity management of its information system, including a list of authorised persons responsible for prevention and timely re-establishment of availability of personal data and access to them in the event of a physical or technical incident.
12. Backup copies and restoring stored personal data (ensuring continuity) - based on risk analysis the controller makes backup copies of personal data at regular intervals. Backup copies are made and tested regularly according to the controller continuity business plan.
13. Archive and data storage - the controller safely performs archiving of personal data that have not yet expired for storage and for which there is no more need for immediate and daily processing. The controller determines the procedure for managing the archived material. The controller must adopt an appropriate document – List (overview) with deadlines for personal data storage – which will contain information about the moment of activation of the period (deadline) for personal data storage, identified periods (deadlines) for personal data storage, the reasons for storing personal data, the legal basis for storing personal data and the data owner.
14. Management of portable media - regarding portable media on which personal data are processed, the controller ensures that they are stored in a location to which only authorised persons determined by the controller have access, and the transfer of media outside the work premises is done only with prior authorisation from the controller. After the transfer of personal data from the media or after the expiration of the specified storage period, the media should be destroyed, erased, or cleared of personal data recorded on it. The controller provides a trace (for example: minutes) for destruction, erasing or cleaning.
15. Encryption of personal data - the controller always applies state of the art technical encryption solutions that ensure integrity, confidentiality, and authenticity of personal data. The controller adopts an internal procedure in which it is obligatory to prescribe the way of managing the secret keys and certificates, considering the risk management of forgotten passwords.
16. Physical security - the controller must apply an enhanced level of security in relation to the premises in which the servers and network equipment are located and stored. If physically located, hosted and administered outside the premises of the controller, the rights and obligations of the controller and the entity or natural person where servers are physically located, hosted and administered, should be regulated by a written agreement.
17. Control of information system and information infrastructure - the documentation for technical and organisational measures must contain the procedures for authorisation of the personal data protection officer ("**DPO**") for performing periodic controls in order to monitor the compliance of the controller with the personal data protection regulations and adopted technical and organisational measures. The information system and information infrastructure of the controller are subject to annual internal control.
18. Managing and hiring processors – the controller is obliged to adhere to the procedure on selection of a processor which is to provide: analysis of potential processor(s) in terms of their technical and organisational measures to ensure that the processing of

personal data will be done in accordance with requirements provided in the personal data protection regulations, as well as for ensuring protection of the rights of personal data subjects; and analysis of the risks to the operation of the controller that may arise from processing of personal data by the processor(s). The mutual rights and obligations of the controller and the processor must be regulated by an agreement whereby the controller, before concluding the contract, is obliged to request the processor to present their security policy based on which processing on behalf of the controller will be done.

II. Standard level of organisational measures:

1. Organisational measures for personal data security (minimum standard) – the employee in charge of human resources at the controller informs the administrator about the employment or engagement of each authorised person with the right of access to the information system in order to be assigned a username and password, as well as for termination of employment or engagement to have his/her username and password deleted.
2. Informing and educating about personal data protection - before starting their work persons who are employed or hired by the controller, are to be acquainted with the regulations for personal data protection, as well as with the adopted technical and organisational measures and personally sign a statement on secrecy and protection of personal data processing, which is required to be kept in the files of persons employed or engaged by the controller.
3. Access to documents - access to documents should be restricted to authorised persons of the controller, while access to documents, mechanisms for identification of authorised persons and categories of personal data to be accessed must be established. If another person needs access to the documents, appropriate procedures should be established for that purpose in the technical and organisational measures.
4. Mandatory application of the “clean desk” rule.
5. Document storage – documents are stored using appropriate mechanisms for prevention of any unauthorised opening. Cabinets, files and other equipment for storing documents must be placed in rooms locked with appropriate protective mechanisms, and when physical characteristics of the premises do not allow it, the controller should apply other measures to prevent any unauthorised access to the documents.
6. Destruction of documents – documents are destroyed by shredding or in another manner which ensures that the same cannot be reused. A report is compiled by a commission and contains all data for complete identification of the document as well as for the categories of personal data contained in it.

III. High level of technical measures:

1. Password management – the controller should use password management tools to secure that different passwords are stored appropriately, whereby it should provide a master password for access to all passwords, which should be enhanced and complex, consisting of a combination of at least 12 alphanumeric characters (letters/lowercase and uppercase/ symbols, numbers and special punctuation signs) and should change after a period not exceeding 30 days.
2. Certification for personal data protection - the controller can, on a voluntary basis, check the processes and internal documents for personal data protection for the purpose of certification of the processes through which personal data are processed. The certification is performed by the Agency or by certification bodies.
3. Management of portable media - the controller is obliged to establish a system for recording the received media in order to enable direct or indirect identification of the type of media received, date and time of receipt, sender, number of media received, type of a document recorded on the media, manner of sending the media, first and last name of the person authorised to receive the media.
4. Certification procedures - the controller may apply other technical measures for confidentiality and protection of personal data processing through the application of certification procedures in accordance with the regulations governing the use of electronic documents, electronic identification, and confidential services.
5. Media transfer - media can only be transmitted outside the workplace if personal data is encrypted or protected by appropriate methods that ensure that the data will not be readable, where only the administrator or a person authorised by it can decrypt it.
6. Transfer of personal data via electronic communications network - personal data may be transmitted over the electronic communications network only if encrypted or specially protected by appropriate methods that ensure that the data will not be legible during transmission.

IV. High level of organisational measures:

1. Copying and duplicating documents - can be done only by authorised persons identified by the controller. Destroying copies or duplicate documents should be done in a way that will prevent further recovery of the personal data contained therein.
2. Transfer of documents - in case of physical transfer, the controller must take measures to protect them from unauthorised access or handling of personal data contained in the documents being transferred.

3. JOINT CONTROLLERS AND CONTROLLER-PROCESSOR RELATIONSHIP

Where two or more controllers jointly determine the purposes and means of processing, they are considered as joint controllers. Joint controllers should enter into an agreement to regulate their respective responsibilities for compliance with the obligations under the Current Data Protection Law. However, irrespective of the terms of this agreement, the data subject may exercise his/her rights under the Current Data Protection Law in respect of and against each of the joint controllers.

When it comes to the relationship between a data controller and a data processor, a written data processing agreement of the prescribed content should be entered into between them. This agreement should govern relevant characteristics of a particular processing (such as the nature and purpose of the processing, its subject matter and duration, type(s) of processed data and category(ies) of data subjects) and mutual rights and obligations of the parties (e.g. obligation of a data processor to process the data only according to the controller’s documented instructions, to ensure that the persons authorised to process personal data are obliged to keep data confidentiality, etc.).

Further, a data controller should only engage a data processor which provides sufficient guarantees that the appropriate measures shall be undertaken in such a way that the processing shall meet statutory requirements and that the protection of the data subject rights shall be ensured. It is also explicitly envisaged that a processor should not engage another processor (i.e. sub-processor) without prior written authorisation, general or specific, of the data controller.

Further obligations of data controllers and/or data processors are described in items 2-6, items 9-11 and items 13 and 14 in this Section 2.

As a general note it should be emphasised that the Current Data Protection Law contains a provision providing data controllers and data processors an 18-month period from the law’s entry into force (i.e. until August 2021) to harmonise their operations with the law. This

legislative provision is very unusual since it leaves an 18-month loophole in terms of data protection rights given that the Old Data Protection Law ceases to apply as of the day of entry into force of the Current Data Protection Law (as of 24 February 2020).

4. DPOS AND REPRESENTATIVES OF FOREIGN ENTITIES

Unlike the Old Data Protection Law which prescribed that all data controllers must appoint a DPO, under the Current Data Protection Law, the same as under the GDPR, data controllers and data processors are obliged to appoint a DPO in certain cases. These are the following:

1. Processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
2. Core activities of the data controller/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; and
3. Core activities of the data controller/processor consist of processing on a large scale of so-called special categories of data and personal data relating to criminal convictions and offences.

The DPO can be an employee of a data controller/processor or an externally/contractually engaged person, whereas legal entities which can be regarded as part of the same group of business subjects can have one joint DPO (under condition that he/she would be equally available to each member of the respective group).

If the DPO is appointed (and such appointment is obligatory only in 3 above-stated cases, while it is voluntary in all other cases), the DPO's contact details should be published and communicated to the Agency. The DPO may fulfil other tasks and duties which do not result in a conflict of interests and reports directly to the highest management of the controller or the processor.

The DPO's duties include, but are not limited to:

1. Inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to the Current Data Protection Law;
2. Monitor compliance with the Current Data Protection Law and with the policies of the controller or processor in relation to the protection of personal data;
3. Cooperate with the Agency and act as the contact point for the Agency on issues relating to processing, including the prior consultation.

The Current Data Protection Law envisages that the DPO should fulfil the following conditions for appointment:

1. Employment conditions determined by the Current Data Protection Law and other laws;
2. Actively use Macedonian language;
3. At the moment of appointment, no penalty or misdemeanour sanction for prohibition to perform a profession, activity or duty is imposed on the person by a final court judgement;
4. Holds a university degree; and
5. Has acquired knowledge and skills in the field of personal data protection practices and regulations in accordance with the provisions of the Current Data Protection Law.

Further, the Current Data Protection Law is applicable to foreign data controllers/processors (extraterritorial effect of the law) in cases when (1) the offering of goods or services is made to subjects in the Republic of North Macedonia, irrespective of whether a payment of the data subject is required, or (2) the monitoring of the data subject's behaviour is conducted, as far as such behaviour takes place within the Republic of North Macedonia.

In such situations the respective foreign entities are obliged to appoint their representatives for the territory of the Republic of North Macedonia. This representative can be either a natural person or legal entity, but it has to be available as the respective foreign entity's contact point in the Republic of North Macedonia to both the Agency and local data subjects.

The rules envisaged by the Current Data Protection Law with regard to both DPOs and representatives are generally aligned with the GDPR.

5. SPECIAL CATEGORIES OF PERSONAL DATA

The Current Data Protection Law recognises special categories of personal data. Their definition and further rules on their processing correspond to the respective GDPR rules.

Under the Current Data Protection Law, the same as under the GDPR, special categories of personal data include data revealing racial or ethnic origin, political opinion, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health and data concerning a natural person's sex life or sexual orientation. In comparison to the Old Data Protection Law (which recognised so-called particularly sensitive data), biometric and genetic data are completely new types of personal data which were not governed by the Old Data Protection Law at all.

Any processing of special categories of data is generally prohibited. However, certain exceptions exist – their processing is allowed in the exceptional cases explicitly prescribed by both the Current Data Protection Law and GDPR. For example, the respective processing is allowed if the data subject has given explicit consent to the processing of such personal data for one or more specified purposes, or if the processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law, or if the processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent, or if it relates to personal data which are manifestly made public by the data subject, or if it is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity, or if it is necessary for reasons of substantial public interest, and in other cases prescribed by the law ("**Exceptional Cases**").

This further means that if a particular processing of the respective data cannot be regarded as one of the Exceptional Cases, it should be regarded as prohibited. Additionally, any processing of the respective data, when allowed, is subject to various additional obligations of data controllers/processors involved in their processing (e.g. potentially applicable obligation of conducting data protection impact assessment).

As a last point, it should also be noted that under the Current Data Protection Law, the following categories of data can only be processed upon obtaining prior written approval from the Agency: (1) data relating to human health, (2) genetic data, unless the data processing is performed by professionals for the needs of preventive medicine, medical diagnosis or care and therapy of the data subject, and (3) biometric data.

The Agency decides on the request for approval within 90 days from the receipt of the request.

6. PROCESSING OF THE DATA SUBJECT'S PERSONAL IDENTIFICATION NUMBER

A data subject's personal identification number can be processed only:

1. Upon prior explicit consent by the data subject (the Agency's prior written approval would be needed if a systematic and extensive processing is done under this basis);

2. For exercise of legally determined rights or obligations of the data subject or controller; and
3. In other cases, as determined by the law.

In cases where the Agency's prior approval for processing of a data subject's personal identification number is needed, the Agency decides within 90 days from receiving the request for approval.

7. DATA PROCESSING AND FREEDOM OF SPEECH AND INFORMATION

The Current Data Protection Law envisages that the application of a wide part of its provisions can be excluded if this is necessary for the purpose of balancing the right to data protection and the freedom of speech and information, and especially in the processing of personal data in the audio-visual area, news archives and press libraries.

The provisions of the Current Data Protection Law referring to the rights of personal data subjects will not apply to the processing of personal data for journalistic purposes only if the public interest prevails over the private interest of the data subject.

8. RIGHTS OF DATA SUBJECTS

The Current Data Protection Law envisages a set of data processing related rights. Their exercise may be conditioned upon fulfilment of certain requirements and/or may be limited depending on the circumstances of each particular case. The law explicitly governs such requirements/limitations as well ("**Prescribed Restrictions**").

In general, subject to the Prescribed Restrictions, these are the following rights: (1) right to request information on a particular processing, (2) right to access to the processed data and to obtain their copy, (3) right to rectification, (4) right to erasure (right to be forgotten), (5) right to restriction of the data processing (e.g. if the processed data's accuracy is contested by the data subject), (6) right to data portability (i.e. right to receive the processed data from the data controller in a structured, commonly used and machine-readable format, as well as to transmit them or to have them transmitted from one controller to the other), (7) right to object to the data processing (e.g. if the processing is based on the legitimate interest or carried out for direct marketing purposes) and to the processing cessation, (8) right to withdraw consent (where consent is a legal ground for the processing), and (9) right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning the data subject or significantly affects him/her ("**Relevant Rights**").

The majority of the Relevant Rights have already been recognised by the Old Data Protection Law, but some of them are completely new (e.g. right to data portability). In any case, data controllers are obliged to ensure exercise of the Relevant Rights (subject to the Prescribed Restrictions) and to do so within exact terms explicitly prescribed by the Current Data Protection Law (i.e. within 30-day period/up to 90-day period if extension of 60 days is necessary due to complexity and number of the requests for the exercise of the respective rights). If they fail to fulfil their statutory obligation or comply with the relevant timeline, data subjects are entitled to file a complaint with the Agency ("**Data Processing Complaint**"). Also, any person who considers that any of his/her rights was infringed by processing activities of a data controller/processor is entitled to the court protection of his/her rights.

The above-described concept of the respective rights is aligned with the GDPR.

9. PROVIDING PERSONAL DATA TO RECIPIENTS

Recipients are defined by the Current Data Protection Law as "natural person or legal entity, public authority, state body or legal entity established by the state for performing public authorisations, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with the law shall not be regarded as recipients; the processing of those data by those public authorities shall be compliant with the applicable data protection rules according to the purposes of the processing".

Data controllers are allowed to provide the personal data for use by recipients for a particular case, if applicable, on the basis of a request submitted by the recipient in writing (or by electronic means), and only if the recipient is allowed to process the data by the law. However, if the law provides for an obligation to provide personal data to the recipient and the same is performed with foreseen dynamics, the recipient does not submit a request to the controller.

The controller is obliged to keep separate records for the categories of personal data provided to recipients, the recipient, legal basis and reason why the personal data was provided, etc.

These rules also apply to situations when personal data is exchanged between government authorities and bodies, unless otherwise provided by the law.

10. RECORDS OF PROCESSING ACTIVITIES AND REGISTRY OF DATABASES

The obligation of keeping records of data processing activities is envisaged by both the Current Data Protection Law and GDPR.

Under the respective regulations, these records should be established in a written form (including also electronic form) and should be kept permanently. They should also be made available to the Agency upon request.

Their content is explicitly prescribed. Specifically, the following information on the processing should be included in these records: name and contact details of the data controller/processor, its DPO if established, purpose(s) of the data processing, type of processed data, category of data subjects, information (and related documents, if applicable) on the processed data transfer out of the economy, general description, where possible, of the security measures undertaken for the protection of the processed data, and certain other information explicitly prescribed by the law.

However, this obligation is not an obligation generally applicable to all data controllers and data processors. It applies only if data controllers/processors have at least 50 employees or, regardless of the number of their employees, if the processing is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data or personal data relating to criminal convictions and offences.

On the other hand, the Current Data Protection Law, unlike the GDPR, envisages the obligation of database registration. Specifically, prior to the adoption of the Current Data Protection Law, data controllers/processors had an obligation to register their databases containing personal data in the Central Registry of Personal Databases ("**Registry**") maintained by the Agency. With the adoption of the Current Data Protection Law, this Registry continues to exist and be maintained by the Agency, but as the registry of databases involving a high risk ("**High-Risk Records**"), whereas controllers/processors should notify the Agency about their respective databases. It is also envisaged that the provisions of the law governing the High-Risk Records shall cease to apply upon accession of the Republic of North Macedonia to the European Union.

11. DATA BREACH RELATED NOTIFICATIONS AND DATA PROTECTION IMPACT ASSESSMENT

Both the obligations regarding data breach related notifications and data protection impact assessment are novelties introduced by the Current Data Protection Law in line with the GDPR. None of them was envisaged by the Old Data Protection Law.

The fulfilment of these obligations depends on the fact whether a particular processing (or a data breach) is likely to result in a risk or high risk to the rights and freedoms of natural persons. If such risk would exist in a particular case, a data controller would be obliged to act as follows: (1) to notify (without undue delay or, if possible, within 72 hours) the Agency and/or data subject of a particular data breach (e.g. if an unauthorised person has accessed the processed personal data and made them available to general public), and (2) to carry out the assessment of an impact which a particular processing could have on the protection of personal data, prior to commencing such processing, whereas it is prescribed that the Agency shall establish and publish a list of the processing operations for which this assessment is required ("**Obligatory Assessment List**"). The Obligatory Assessment List has already been established – it is envisaged by one of the bylaws adopted upon enactment of the Current Data Protection Law (more information on this bylaw and other secondary legislation adopted in relation to the Current Data Protection Law is provided under item 17 below).

Also, when it comes to a data breach, a data processor is obliged to notify a data controller of a data breach without undue delay after becoming aware of the same.

12. CODES OF CONDUCT AND CERTIFICATION

Associations and other bodies representing categories of data controllers or data processors, in line with the specific characteristics of different data processing sectors and needs of micro, small and medium-sized enterprises, can prepare/amend/extend codes of conduct in order to specify the implementation of the Current Data Protection Law.

The (amended/extended) code of conduct is delivered to the Agency for its opinion and approval. The Agency will keep a registry of approved codes of conduct – this matter will be regulated by a dedicated bylaw.

The monitoring over the codes of conduct can be performed by a body accredited by the Agency for monitoring of the compliance of codes of conduct. Detailed standards and norms for accreditation are yet to be prescribed.

In line with the specific characteristics of different data processing sectors and needs of micro, small and medium-sized enterprises, in order to contribute to the rightful implementation of the Current Data Protection Law, the Agency encourages the establishment of data protection certification mechanisms and of data protection seals and marks. The certification is voluntary and publicly available.

However, the certification does not reduce the responsibility of the controller and the processor and does not exclude the Agency's competences.

The certification is performed by the Agency or certification bodies accredited in line with the standards and norms which are yet to be prescribed. The certification bodies will be accredited by the Accreditation Institute of the Republic of North Macedonia. The same rules will apply to certification of bodies for performing data protection training.

The certificate issued to the data controller will be valid for a period of 3 years and can be renewed under the same conditions if the prescribed standards and norms are fulfilled.

The Agency will keep a registry of all certification mechanisms and all data protection seals and marks – this matter will be regulated by a dedicated bylaw.

The compliance with the approved codes of conduct or the approved certification mechanisms can be used as an element to prove the compliance of the controller with its data protection obligations.

13. DATA TRANSFER

Where the data protection legislation of the Republic of North Macedonia differs perhaps the most from the GDPR is the topic of data transfer. This is due to the fact that the Current Data Protection Law provides for (1) specific cross-border/boundary transfer requirements and that (2) data transfers from North Macedonia to EU/EEA member states are subject to notification to the Agency.

Specifically, a prior approval by the Agency ("**Transfer Approval**") is required for cross-border/boundary data transfers to economies outside EU/EEA. The Transfer Approval may be provided based on either an adequacy decision issued by the Agency for the (importing) third economy or international organisation ("**Adequacy Decision**") or if appropriate safeguards are provided.

The appropriate safeguards may be provided by:

1. A legally binding and enforceable instrument between public authorities or bodies;
2. Binding corporate rules in accordance with the Current Data Protection Law;
3. Standard data protection clauses determined by the Agency or approved by the European Commission;
4. An approved code of conduct or approved certification mechanism pursuant to the Current Data Protection Law together with binding and enforceable commitments of the controller or processor in the third economy to apply the appropriate safeguards, including as regards the data subject's rights.

Additionally, the Agency could approve the following appropriate safeguards:

1. Contractual clauses between the data controller and the data processor, as well as the data controller, the data processor or the recipient of the personal data in the third economy or international organisation; or
2. Provisions envisaged in administrative agreements between public authorities or bodies which contain applicable and effective data subject rights.

The Current Data Protection Law also provides a list of derogations for specific situations, based on which a legitimate data transfer out of the Republic of North Macedonia is not conditioned upon a Transfer Approval (e.g. data subject's consent, enforcement of a contract between a data subject and a data controller, etc.). However, up until this moment, the Agency has had a very conservative approach and has insisted that even in such cases a Transfer Approval has to be obtained. We understand from unofficial consultations with the Agency's officials that the practice of the Agency in this respect (in light of the Current Data Protection Law) is not likely to change.

In this regard, it should be noted that the Current Data Protection Law itself does not require a special/individual Transfer Approval from the Agency if the Adequacy Decision exists or the above-described safeguards are provided. However, in line with the initial informal consultations with the Agency, the Agency's interpretation is that such Transfer Approval will be necessary for cross-border/boundary data transfers to economies outside EU/EEA.

The Agency decides upon the request to issue a Transfer Approval within 90 days from receipt of the request. The controller can submit a lawsuit against the decision of the Agency before the Administrative Court of the Republic of North Macedonia within 30 days from its receipt.

14. VIDEO SURVEILLANCE

Video surveillance should be limited to a part of the premises which is necessary to be under the video-surveillance for the sake of fulfilling the purposes for which the respective surveillance is set. The data controller may conduct video surveillance in the business premises if necessary to: protect the life and health of people, protect the property, protect the life and health of employees due to the nature of their work, or provide control of

entry and exit from the business premises only for safety purposes. Video surveillance in wardrobes, dressing rooms, toilets, and other similar premises is prohibited. The controller is obliged to notify the employees about video surveillance in official or business premises.

Video recordings are kept until the purposes for video surveillance are fulfilled, but not longer than 30 days, unless a specific law envisages a longer period.

The controller should conduct analysis of the purpose(s) for which the video surveillance will be established before starting the process of establishing a video surveillance system.

The controller is obliged to evaluate the results of video surveillance system every 2 years and prepare a report as an integral part of the documentation for establishing a video surveillance system.

A notification containing the following information should be placed in the premises where video surveillance is conducted:

1. That video surveillance is carried out,
2. The name of the controller performing the video surveillance, and
3. The way information can be obtained about where and how long the recordings of the video surveillance system are stored.

The data controller is obliged to regulate the manner of conducting video surveillance by an internal act.

A written statement of consent of at least 70% of the total number of owners, residents/tenants of the apartments is required to conduct video surveillance in residential buildings. The Current Data Protection Law prohibits recording of entrances of individual apartments. Also, it is prohibited to transmit the recordings from the video surveillance in residential buildings through cable television (public or internal network), via the Internet or other electronic means of data transmission.

15. SUPERVISION AND DATA SUBJECT'S RIGHTS TO REMEDY

The Agency supervises the implementation of the Current Data Protection Law. The authorised supervisors in the Agency can perform regular, extraordinary and control supervision over controllers and processors, impose corrective measures on the controlled entity and initiate misdemeanour proceedings.

Data subjects have the right to lodge a complaint with the Agency if the data subject considers that the processing of personal data relating to him/her infringes the Current Data Protection Law.

Without prejudice to any available administrative or non-judicial remedy, each data subject has the right to an effective judicial remedy where he/she considers that his/her rights under the Current Data Protection Law have been infringed as a result of the processing of his/her personal data in non-compliance with the Current Data Protection Law.

Any person can request compensation of (material or non-material) damages which occurred due to infringement of the Current Data Protection Law by submitting a lawsuit against the data controller or data processor before the competent court.

16. PENAL POLICY

The Current Data Protection Law, much like the GDPR, imposes fines in the amount of up to 2% and up to 4% of the total annual turnover of the preceding financial year upon controllers and processors and legal entities in case of non-compliance with the Current Data Protection Law. Responsible persons in legal entities can be fined between EUR 300 and EUR 500.

Additionally, the Current Data Protection Law stipulates a fine in the range between EUR 1,000 and 10,000 for controllers (legal entities) that do not follow the requirements for video surveillance, while responsible persons in legal entities can be fined between EUR 100 and EUR 500.

In comparison, the Old Data Protection Law provided for much lighter penalties ranging up to EUR 2,000 for the breaching entity and up to EUR 600 for the entity's responsible person.

17. RELEVANT SECONDARY LEGISLATION

In addition to the Current Data Protection Law, a total of 13 secondary legislation acts were adopted by the Agency in May 2020, as follows:

1. **Rulebook on the Personal Data Transfer** - This rulebook regulates the manner in which the controller/processor notifies the Agency of a data transfer to the member states of the European Union/European Economic Area, as well as the application form used to submit such notification to the Agency. Additionally, it regulates the content of the application form used by controller/processor to request the Transfer Approval when such approval is needed. Specifically, the rulebook provides the form for requesting Transfer Approval on the basis of an adequacy decision, appropriate safeguards, or binding corporate rules. The rules on keeping records of conducted data transfers kept by the Agency are also governed by this rulebook. Having in mind that this rulebook envisages notifying the Agency of data transfers to member states of the European Union/European Economic Area, as well as obtaining a Transfer Approval in situations not envisaged by the GDPR (e.g. on the basis of an adequacy decision adopted by the Agency), this rulebook is not entirely GDPR compliant;
2. **Rulebook on the Personal Data Protection Training** - This rulebook regulates the ways in which the Agency may organise training for controllers'/processors' employees and for DPOs. The costs of training are borne by the participants. At the end of the training, the participants receive a certificate valid for 3 years. The training is established in accordance with the Annual Programme for Personal Data Protection Training. The application for and the form and content of certificates issued to participants, as well as the method of keeping records of certificates issued are prescribed by this rulebook. Although the GDPR does not have a similar provision, it prescribes as one of the tasks of the European Data Protection Board to promote common training programmes and facilitate personnel exchanges between the supervisory authorities, which suggests that the types of training as envisaged by this rulebook are not contrary to the GDPR;
3. **Rulebook on the Form and Content of the Request for Determining the Violation of the Provisions of the Law on Personal Data Protection** - The form and content of the respective request are prescribed by this rulebook. This rulebook is GDPR compliant;
4. **Rulebook on the Safety of Personal Data Processing** - This rulebook provides guidelines which controllers must follow when they implement measures for ensuring safety of the processed data and defines two levels of such measures (standard and high). It further regulates which technical and organisational measures must be implemented under each security level. Standard level technical measures include: authentication of authorised persons, securing the equipment used for personal data processing, segregation of duties and responsibilities, control of access to the information system, access logs, securing the portable media, protection of internal network, securing of the servers, securing the website of the controller, obligations and duties of the administrator of the information system and authorised persons, prevention, reaction and rehabilitation of incidents, backup copies and recovery of personal data, method of archiving and storing personal data, managing portable media, encrypting personal data, physical safety, control of the information system

and information infrastructure, managing the processors, engaging processors. Standard level organisational measures include: organisational measures for personal data safety (minimal standard), informing and educating on personal data protection, access to documents, "clean desk" rule, destroying documents, method of keeping the documents. High level technical measures include: additional measures, password management, managing portable media, certification procedures, transfer of media, transfer of personal data through an electronic communication network. High level organisational measures include: copying and multiplication of documents, transfer of documents. These measures are described in more detail in Section 2, item 2 herein. We find that this rulebook is GDPR compliant and it regulates this matter in more detail than the GDPR;

5. **Rulebook on the Content of Analysis of Video Surveillance Purposes and Report on the Periodic Evaluation of Video Surveillance System** - This rulebook provides that data controllers which conduct video surveillance are obliged to perform the analysis of respective processing and its periodical evaluation, both in the prescribed form and content. After the analysis is conducted, it is submitted to the DPO to provide its opinion. Based on this, the responsible person of the data controller adopts a decision on conducting video surveillance. The GDPR does not include provisions on video surveillance, however, we find that this rulebook is generally in line with the GDPR's principles and provisions;

6. **Rulebook on the Content and Form of the Act on Conducting Video Surveillance** - This rulebook prescribes the act on the manner in which the video surveillance is to be performed and should be adopted by data controllers. It additionally provides for a template warning sign, authorisation for processing personal data through the video surveillance system, statement for securing safety of the data processing, and privacy notice when conducting video surveillance. The GDPR does not include provisions on video surveillance, however, we find that this rulebook is generally in line with the GDPR's principles and provisions, as well as the Guidelines 3/2019 on processing of personal data through video devices dated 10 July 2019 of the Working Group 29 of the European Union;

7. **Rulebook on the Form and Content of Official ID Card and Its Issuance and Revocation** - This rulebook prescribes the form and content of the official ID Card of supervisors (who are administrative officers of the Agency authorised to conduct supervision over the legality of activities undertaken for the purposes of personal data processing, as well as implement the Current Data Protection Law and its bylaws). The Agency keeps records of each issued, revoked, replaced, destroyed or lost ID Card. This matter is not specifically regulated with the GDPR;

8. **Rulebook on Supervision Method** - This rulebook regulates the method of supervision conducted by the supervisor for personal data protection, as well as the method of keeping records for the supervision. The supervision is conducted in accordance with the Annual Programme for Supervision and monthly supervision plans adopted by the Agency. Before starting the supervision, the supervisor carries out preparatory activities. The supervision can be: (i) regular (where the operations of the controller are under revision); (ii) extraordinary (an investigation for identifying flaws and weaknesses of the controller's system for collecting, processing and keeping of personal data) and (iii) control supervision. The supervision may be announced or unannounced, complete or partial, and is conducted at the premises of the controller and the Agency. We find that this rulebook is GDPR compliant and it regulates this matter in more detail than the GDPR;

9. **Rulebook on the Data Breach Notification Method** - This rulebook governs the procedure for notifying the Agency (via e-mail or through the website https://eprijavi.privacy.mk/) and data subjects of a data breach including also the form and content of such notification. The controller is obliged to record all violations of personal data which have occurred, including the facts, consequences and measures undertaken. An internal system for recording the violations must also be established, regardless whether the Agency should be notified or not. The DPO must be informed and included in the process of handling and notifying of the violation in order to provide adequate advice and monitor whether this process is in line with the Current Data Protection Law and applicable data protection regulations. This rulebook is GDPR compliant and is adopted in relation to the Guidelines on Personal data breach notification under Regulation 2016/679 (wp250rev.01) of the Working Group 29 of the European Union;

10. **Regulations regarding data protection impact assessment** (i.e. Rulebook on the Process of Data Protection Impact Assessment and Lists of the Types of Processing Operations for which the Data Protection Impact Assessment is/is not required) - These regulations govern the guidelines which a data controller needs to consider when it conducts data protection impact assessment (DPIA), certain other relevant issues with respect to the DPIA (such as, for example, its methodology and publication), as well as cases when the DPIA's performance is obligatory/non-obligatory. The DPIA must be prepared prior to the processing of personal data, while providing data protection by design and by default. The data controller is solely responsible for the preparation of DPIA. However, the controller may engage external persons for the preparation of the DPIA or consult independent experts and request their opinion or advice. Each phase of DPIA needs to be documented by the data controller, who then prepares a report. This report includes: (i) description of the processing; (ii) internal and external persons included in the DPIA process; (iii) risk analysis; (iv) measures for risk management; (v) conclusion; (vi) action plan; (vii) opinion of the DPO and other persons included in the DPIA process; and (viii) approval of the responsible person of the controller. These regulations are GDPR compliant and are adopted in relation to the Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP248 rev.01 of the Working Group 29 of the European Union;

11. **Rulebook on the Notification of the High-Risk Data Processing** - This rulebook governs rules on the High-Risk Records, as defined under Section 2, item 10 herein, in that it stipulated the manner in which a data controller notifies the Agency of its data processing activities which pose high risk to the rights and freedoms of data subjects. The Agency prescribes a dedicated notification form, which the controller submits electronically through the Agency website in order to be recorded in the High-Risk Records. This rulebook is not compliant with the GDPR as the GDPR does not envisage such obligations for data controllers.

3. COMPETENCE OF AND CHALLENGES IN THE WORK OF THE AGENCY

The public authority with the competence in the field of data protection is the Agency for Personal Data Protection of the Republic of North Macedonia (in Macedonian: *Агенција за заштита на лични податоци*).

The Agency is an autonomous public authority established in 2005. Under the Current Data Protection Law, the Agency is declared to be completely independent in preforming its work and authorisations, free of any, direct or indirect, external influence and cannot request or receive orders from anyone. The Agency is accountable for its work before the Assembly of the Republic of North Macedonia.

The Agency is managed by the Director who is elected and dismissed by the Assembly of North Macedonia. The Deputy Director of the Agency is also elected and dismissed by the Assembly.

The funds for Agency's operations are obtained from the budget of the Republic of North Macedonia. In addition, the Agency can have its own income from fees it charges (e.g. for accreditation, certification, opinions for accreditation, training, etc.), donations and other sources. This income can be used to cover the expenses of investments and current operations, professional development and training of employees, as well as for performing other activities in accordance with the provisions of the Current Data Protection Law.

The material and financial operations of the Agency are audited by the State Audit Office of the Republic of North Macedonia.

Even though the Current Data Protection Law provides that the Agency has full political, financial and functional independence, this is not fully implemented in practice. The employment and promotion process in the Agency is not entirely vested in the Agency, but includes involvement of the Agency for Administration of the Republic of North Macedonia and the Ministry of Finance. The initial draft Law for Protection of Personal Data dated December 2018 ("**Draft Law**", https://ener.gov.mk/Default.aspx?item=pub_regulation&subitem=view_reg_detail&itemid=49944) envisaged that the Agency Director decides about employment and promotion in the Agency, within the framework of funds allocated to the Agency from the government budget, without prior consent or opinion as envisaged by the law. However, this provision was not accepted and is not part of the Current Data Protection Law. This is a challenge for the Agency, especially considering its supervisory powers over the public sector institutions in the data protection area, some of which are involved in its recruiting process.

Another provision which was included in the Draft Law and was not accepted as integral part of the Current Data Protection Law is the provision regulating the salary of Agency employees. In line with the Draft Law, due to the specific authorisations and responsibilities of the Agency employees, their basic salary and their salary supplement for title is increased by 33%, and Agency employees could receive monetary awards and bonuses in case of achieved exceptional results in their work. However, stakeholders did not accept such provision. The salary issue is a great challenge for the Agency and can lead to outflow of trained Agency professionals to the private sector.

During our discussions, Mr. Igor Kuzevski, Deputy Director of the Agency confirmed this. For Mr. Kuzevski it is of outmost importance that the salary issue is dealt with as soon as possible in order to prevent the outflow of professionals, especially considering that most of them have new and more complicated roles under the Current Data Protection Law, which includes issuing fines for misdemeanours which are far from symbolic. Mr. Kuzevski informed us that a new functional analysis has been prepared and a new job systematisation is being developed, which is expected to enter into force from 1 January 2021.

The Agency's competences are set in detail by the Current Data Protection Law (e.g. prepares and adopts bylaws related to personal data protection; develops policies and provides guidance on personal data protection; conducts inspections; assesses the legality of processing of personal data; keeps a register; issues approvals for processing of personal data; issues prohibitions on further processing of personal data by the controller; authorises the transfer of personal data to other economies; gives opinions on draft laws in the field of personal data protection; gives opinions on draft codes of conduct related to personal data protection; conducts misdemeanour proceedings; acts upon requests of supervisory bodies in the field of personal data protection of other economies in relation to the performance of their activities on the territory of the Republic of North Macedonia; delivers training and provides technical assistance to interested controllers/processors, etc.).

For the purpose of exercising the authorisations and duties within its sphere of competence, the Agency has two types of powers: (1) powers relating to its capacity of a second-instance authority responsible for protecting the right to data protection in appeal proceedings (i.e. based on the Data Processing Complaints filed with the Agency) ("**Appeal Related Powers**") and (2) powers relating to its capacity of a supervisory authority responsible for enforcing the Current Data Protection Law ("**Supervisory Powers**").

When it comes to the Agency's Appeal Related Powers, it decides on filed complaints within 30 days from the day of their filing, whereas it firstly forwards the complaints to the data controller(s) responsible for undertaking data processing activities which the complaints were filed against for their comments. Depending on whether the Agency finds a complaint grounded, it may reject it (if ungrounded) or order the data controller to act upon the request within a specified period of time (if grounded). In any case, no appeal can be filed against a decision passed by the Agency, but an administrative dispute can be initiated against such decision (or if the Agency does not pass a decision within the statutory term) before the competent court.

When it comes to the Agency's Supervisory Powers, the Agency is entitled, amongst other, to order certain corrective measures to data controllers/processors (e.g. to order them to stop undertaking particular data processing activities), as well as to file a request for initiating offence proceedings against them before the competent court. Additionally, the Current Data Protection Law also establishes the Agency's competence to issue fines for all offences directly based on the Current Data Protection Law.

Other government authorities and bodies are obliged to notify the Agency of the measures undertaken for implementation of the requests, proposals, opinions, recommendations or indications made by the Agency, within the deadline specified by the Agency, but no later than 30 days from the day of receipt of the request submitted by the Agency.

The support (other than the regular budget support) the Agency (potentially) receives for the purpose of further development of data protection policies and practice in the Republic of North Macedonia is very important as regards its work and organisation. Based on the information publicly available on the Agency's website, the Agency participated in a few important and successfully implemented projects in the period from 2010 to 2018. These are:

1. **Support to Access to Right of Personal Data Protection" Europeaid/135668/IH/SER/MK - The European Union IPA TAIB 2012 Programme**[16] which is the EU-funded project implemented between November 2015 and October 2017 and aimed to further improve the overall legal and institutional framework for data protection in line with the EU best practices in order to ensure that individuals can exercise their data protection rights effectively;
2. **Procurement of Equipment for the Agency for Personal Data Protection**[17] financially supported by the European Union within the IPA TAIB 2012 programme and implemented over a period of 7 months in the course of 2016. This project was centred around the procurement of ICT equipment (hardware and software) to modernise the work of the Agency and improve e-services to citizens and data controllers/processors;

16 https://dzlp.mk/mk/node/3131

17 https://dzlp.mk/mk/content/%D0%BD%D0%B0%D0%B1%D0%B0%D0%B2%D0%BA%D0%B0-%D0%BD%D0%B0-%D0%BE%D0%BF%D1%80%D0%B5%D0%BC%D0%B0-%D0%B7%D0%B0-%D0%B4%D0%B8%D1%80%D0%B5%D0%BA%D1%86%D0%B8%D1%98%D0%B0%D1%82%D0%B0-%D0%B7%D0%B0-%D0%B7%D0%B0%D1%88%D1%82%D0%B8%D1%82%D0%B0-%D0%BD%D0%B0-%D0%BB%D0%B8%D1%87%D0%BD%D0%B8%D1%82%D0%B5-%D0%BF%D0%BE%D0%B4%D0%B0%D1%82%D0%BE%D1%86%D0%B8

3. **Sustainable System for Continuous Education on the Data Protection Principles in Primary and Secondary Education - IPA / TAIB2009 / 4.2 / LOT7 / 05**[18] implemented in 2013 and 2014 with the objective of achieving the higher level of awareness of personal data protection and student privacy, as one of the fundamental and most important human rights;
4. **Support in the Preparation of Strategic Documents and Appropriate Action Plans, including Research of Media Awareness for Implementation of the Right to Data Protection**[19] implemented in the period from March until December 2011, financed by the IPA 2008, Component 1, and aimed at strengthening the powers of the Agency, improving the implementation of legislation in the field of personal data, and raising public awareness about their right to protection of personal data;
5. **Technical Assistance for Strengthening Organisational and Institutional Capacities for Personal Data Protection**[20] implemented with the support from the Norwegian Personal Data Protection Authority (NorSIS). The objective was to create better mechanisms for personal data protection on social networks, to strengthen awareness of privacy and technological development, as well as to strengthen the capacity of the Agency by providing a more efficient way for the protection of personal data on the Internet and social networks;
6. **Continuous Support for the Improvement of the Personal Data Protection System**[21] supported by NorSIS with the objective of introducing new mechanisms and tools in the existing legal environment, paying special attention to particular issues such as data processing in cloud computing.

Currently, there is potential IPA Twinning project in the pipeline, however, it is yet to be seen whether North Macedonia will take part in it.

According to the Agency's website[22], the Agency has so far signed 14 Declarations on Cooperation with Personal Data Protection Authorities from Bulgaria, Montenegro, Germany (Berlin), Denmark, Lithuania, Poland, Romania, Croatia, Italy, Slovenia, Czech Republic, Russia, Kosovo* and Estonia. The Agency also published that it is an equal voting member of the Consultative Committee (T-PD) of the Council of Europe of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, the European Conference on Personal Data Protection (Spring Conference), the Central Conference and the Eastern European Data Protection Authorities, the Police and Judiciary Working Group, the International Conference of Commissioners for Personal Data Protection and Rivalry, the International Working Group on Personal Data Protection in the field of telecommunications, case handling workshops and that it has observer status in Working Group 29 of the European Union.

Mr. Igor Kuzevski, Deputy Director of the Agency, informed that the Agency has strong cooperation with the data protection authority of Switzerland.

18 https://dzlp.mk/node/2144

19 https://dzlp.mk/node/2146

20 https://dzlp.mk/mk/content/%D1%82%D0%B5%D1%85%D0%BD%D0%B8%D1%87%D0%BA%D0%B0-%D0%BF%D0%BE%D0%BC%D0%BE%D1%88-%D0%B7%D0%B0-%D0%B7%D0%B0%D1%98%D0%B0%D0%BA%D0%BD%D1%83%D0%B2%D0%B0%D1%9A%D0%B5-%D0%BD%D0%B0-%D0%BE%D1%80%D0%B3%D0%B0%D0%BD%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%81%D0%BA%D0%B8%D1%82%D0%B5-%D0%B8-%D0%B8%D0%BD%D1%81%D1%82%D0%B8%D1%82%D1%83%D1%86%D0%B8%D0%BE%D0%BD%D0%B0%D0%BB%D0%BD%D0%B8%D1%82%D0%B5-%D0%BA%D0%B0%D0%BF%D0%B0%D1%86%D0%B8%D1%82%D0%B5%D1%82%D0%B8-%D0%B7%D0%B0-%D0%B7%D0%B0%D1%88%D1%82%D0%B8%D1%82%D0%B0

21 https://dzlp.mk/mk/node/2981

22 https://dzlp.mk/mk/msorabotka

The Strategy for Implementation of the Right to Personal Data Protection in the Republic of North Macedonia 2017 – 2022 ("**2017-2022 Strategy**", available at: https://dzlp.mk/sites/default/files/u4/dpdp_strategy_v1_en_16.01.2017_web.pdf) prepared within the framework of Support to Access to Right of Personal Data Protection" Europeaid/135668/IH/SER/MK - The European Union IPA TAIB 2012 Programme defined the following strategic goals:

1. Goal 1 - The Republic of North Macedonia to be recognised as a state which provides an adequate level of personal data protection;
2. Goal 2 - Establishment of a self-sustainable system for personal data protection;
3. Goal 3 - Continuous increase of public awareness on and culture of personal data protection;
4. Goal 4 - Continuous improvement of the compliance of data controllers and data processors;
5. Goal 5 - Continuous cooperation with partners;
6. Goal 6 - Increasing the efficiency of administrative procedures;
7. Goal 7 - Effective handling of international issues;
8. Goal 8 - Trained and motivated team ready to respond to challenges.

The strategic goal 1 ("The Republic of North Macedonia to be recognised as a state which provides an adequate level of personal data protection") would include:

1. Adoption of an adequacy decision by the European Commission that the Republic of North Macedonia has an adequate level of data protection;
2. Harmonisation of the legislation: the Current Data Protection Law with the GDPR (this was done in February 2020 with the adoption of the Current Data Protection Law which is largely harmonised with the GDPR), harmonising the secondary and sector legislation with the Current Data Protection Law, adaptation of relevant internal acts.

The strategic goal 2 (establishment of a self-sustainable system for personal data protection) would include:

1. Strengthening the position of the Agency as an independent supervisory body (in accordance with the independence criterion based on Article 52 of the GDPR);
2. The Agency to obtain the status of a certification body (in accordance with the Current Data Protection Law, based on Article 42-43 of the GDPR);
3. Strengthening the position of DPOs (in accordance with the Current Data Protection Law, as well as providing support, training, etc.).

The strategic goal 3 (continuous increase of public awareness on and culture of personal data protection) would include:

1. Increased level of knowledge of citizens about their rights to personal data protection (a separate communication strategy is envisaged to support this activity);
2. Increased level of enforced decisions, which requires an increased number of conducted control supervisions;
3. Adoption of sectoral codes of conduct for protection of personal data, as a tool that supports self-regulation aimed at the compliance of certain sectors.

The strategic goal 4 (continuous improvement of the compliance of data controllers and data processors) would include:

1. Improving accountability tools (impact assessment on personal data protection, design privacy, auditor, etc.), which support controllers/processors to implement a system that complies with the provisions of the Current Data Protection Law.

The strategic goal 5 (continuous cooperation with partners) would include:

1. Increased cooperation with government bodies and private sector;
2. Strengthened cooperation with NGOs.

The strategic goal 6 (increasing the efficiency of administrative procedures) would include:

1. Introduction of new technologies (online inspection, electronic case management, etc.);
2. Strengthening the *ex officio* system for dealing with cases of obvious/determined violation of the Current Data Protection Law;
3. Response in accordance with the quality system.

The strategic goal 7 (effective handling of international issues) would include:

1. Active cooperation with data protection authorities from other economies, the Board and the Commission for international cases (following the new rules of international transfer of personal data).

The strategic goal 8 (trained and motivated team ready to respond to challenges) would include:

1. Trained team - skills development;
2. Motivated team - work environment, employee reward system (inclusion of a wide range of motivation tools).

Within the framework of Support to Access to Right of Personal Data Protection Europeaid/135668/IH/SER/MK - The European Union IPA TAIB 2012 Programme, 2018-2023 Communication Strategy of the Agency ("**Communication Strategy**", https://dzlp.mk/sites/default/files/komunikaciska_strategija_final_printed.pdf) was developed. The Communication Strategy follows directly the 2017-2022 Strategy and supports its implementation.

The strategic communication goals are focused on:

1. Promoting the new European standards for personal data protection (as a key guarantee for privacy protection) to various stakeholders for personal data protection and assistance to achieve the highest level of compliance;
2. Raising awareness of various stakeholders for personal data protection about the importance and practical value of the recognition of the Republic of North Macedonia as an economy that provides an adequate level of personal data protection;
3. Effective communication about the role and mission of the Agency to all stakeholders and strengthening its position as a recognised protector and promoter of the right to personal data protection;
4. Promoting and informing data controllers and data processors as well as the general public about the importance of the position of the DPOs, about the mission and the role they play in the national system for personal data protection;
5. Strengthening the awareness, knowledge and level of information of the DPO in accordance with the new legal framework for personal data protection;
6. Promoting and informing the public about their rights regarding personal data protection as well as the importance of personal data protection, given the new technological challenges and the new legal framework for personal data protection;
7. Implementation of an effective preventive policy for greater compliance with internationally recognised standards and mandatory requirements in the field of personal data protection;

8. Improving the application of self-regulation mechanisms to ensure transparency and security for data controllers, data processors and data subjects;
9. Focusing on the Agency's awareness-raising efforts focused on data controllers and data processors and the importance of different accountability tools;
10. Promoting cooperation with the public, private and civil sector, media, ombudsman and others, on issues and information related to personal data protection in accordance with the legal framework;
11. Education, promotion and awareness raising of young people and children as well as all groups (parents, teachers and professors) involved in the process of educating young people about personal data protection;
12. Promoting the introduction and implementation of new technologies in the basic activities of the Agency aimed at data controllers, data processors and data subjects;
13. Transparency, accountability and responsibility in relation to the operations of the Agency;
14. Strengthened internal communication and involvement of Agency employees in the implementation of the Communication Strategy;
15. Information, communication and cooperation with international institutions, bodies and committees involved in personal data protection activities (the Board, the European Commission, competent supervisory bodies);
16. Encouraging continuous self-education of Agency's employees and implementation of a merit-based human resource management policy to motivate people and ensure sustainability of work results.

In addition to the Agency, other relevant institutions in the data protection area include, but are not limited to:

1. **Assembly of North Macedonia** - The Assembly of North Macedonia is the legislative authority in North Macedonia. It is the authority which adopts the laws in the economy, and as such has adopted the Current Data Protection Law. The Agency is accountable for its work to the Assembly and prepares and submits annual reports about its work to the Assembly. The Assembly also appoints and dismisses the Director of the Agency. Additionally, the Assembly is the only body competent for interpreting laws in North Macedonia by issuing an authentic interpretation.
2. **Ministry of Justice of North Macedonia** - Ministry of Justice of North Macedonia is the authority which prepared the text of the Current Data Protection Law, which was then proposed by the Government (via Minister and Deputy Minister of Justice) for adoption by the Assembly.
3. **Administrative Court of North Macedonia** - Administrative Court of North Macedonia is the judicial authority which decides in first instance in administrative proceedings. In cases where the parties are dissatisfied with the decisions issued by the Agency, they can submit a lawsuit to the Administrative Court within 30 days from the day of receiving the decision. In general, the lawsuit does not prevent the execution of the decision. If the Administrative Court adopts a judgement which leaves the plaintiff dissatisfied, an appeal may be submitted to the Higher Administrative Court of North Macedonia within 15 days as of the day of receiving the judgement. The appeal delays the execution of the appealed judgement.
4. **Constitutional Court of North Macedonia** - Constitutional Court of North Macedonia is the authority which protects the constitutionality and legality and the rights and freedoms of individuals. It is the authority which decides whether the adopted laws

and regulations are in line with the Constitution of North Macedonia. Anyone can submit an initiative to the Constitutional Court to initiate a procedure for assessing the constitutionality of the Current Data Protection Law, or any of its provisions, and whether they are legal and in line with the Constitution of North Macedonia.

5. **Competent courts** - First instance courts in North Macedonia are competent to decide on a lawsuit submitted by a data subject for compensation of damages suffered by the data subject as a result of a breach of the Current Data Protection Law.
6. **Public Prosecutor's Office** - Public Prosecutor's Office is the body that prosecutes perpetrators of crimes, including crimes related to data protection (e.g. abuse of personal data). The Public Prosecutor's Office can be aided by different bodies, e.g. the police (in certain situations the police would aid the Agency as well), etc.
7. **Inspection bodies** - In addition to the authorised supervisors at the Agency, other inspection bodies have competences related to implementation of data protection provisions of different laws and misdemeanours in case of their breach, for example, the labour inspectorate in case of breaching employees' data protection rights by employers, the Agency for Electronic Communications of North Macedonia related to personal data of subscribers of a public electronic communications service, the State Market Inspectorate related to personal data of consumers, the State Election Commission related to protection of personal data of citizens included in the electoral register; etc. Depending on the law that was violated, different bodies are competent to conduct a misdemeanour procedure and in accordance with this, their decisions could be appealed before different secondary instance bodies.

4. CHALLENGES IN THE IMPLEMENTATION OF THE CURRENT DATA PROTECTION LAW IN PRIVATE AND PUBLIC SECTOR

The challenges which are ahead of local entities in both private and public sector are numerous. The most difficult ones are those linked to the full and adequate implementation of the principles of accountability and data protection by design and default.

This is due to the fact that the implementation of respective principles requires from the entities involved in any processing of personal data to respect the data protection requirements (such as, for example, data minimisation) from the very creation/further development of their IT system as, otherwise, they would not be able to respond to or address the challenges which the respective law imposes (such as, for example, the requirement to ensure exercise of the data subject processing related rights and to ensure such exercise is made within the terms envisaged by the law, or requirement to timely prepare and file data breach notifications).

Accordingly, full and adequate implementation of the Current Data Protection Law requires significant investments (e.g. for obtaining adequate equipment/software and hiring qualified personnel) for the vast majority of the respective entities.

Some matters regulated in the Current Data Protection Law cannot be implemented yet since the Agency has not adopted respective bylaws yet. For example, the codes of conduct and certification mechanisms are still not implemented. In line with unofficial communication with authorised persons at the Agency, they have not started working on this matter and will need assistance from European experts in order to adopt the bylaws regulating codes of conduct and certification mechanisms.

Additionally, there is an 18-month period from the entry into force of the Current Data Protection Law (i.e. until 24 August 2021) in which: (i) data controllers, data processors and the Agency have to harmonise their operations with this law; (ii) the envisaged bylaws should be adopted; and (iii) other laws and regulations should be harmonised with the Current Data Protection Law. This gap between the application of the Old Data Protection Law (which ceased to apply on 24 February 2020) and the 18-month period of reaching compliance with the Current Data Protection Law also leads to insufficient enforcement of the Current Data Protection Law.

Another challenge in the implementation of the Current Data Protection Law is the low level of data protection knowledge and experience of employees in public administration bodies, while Agency employees still need to undertake training and better understand the essence of the GDPR, having in mind that economy's goal is to achieve full harmonisation with the European Union legislation. Sector legislation is still not harmonised with the Current Data Protection Law and this process appears to be moving very slowly. The sectoral harmonisation was greatly influenced by the spread of Covid-19 in the economy, causing the process to slow down.

The Old Data Protection Law posed various administrative obligations on data controllers and data processors which included obtaining approvals and making registrations with the Agency, which add to the bureaucratic approach taken by the Agency in its interpretation of the Current Data Protection Law, as well as the approach taken as regards the adopted bylaws. For example, the Current Data Protection Law itself does not require a special/individual transfer approval from the Agency if an adequacy decision was issued by the Agency for the (importing) third economy or international organisation or if appropriate safeguards are provided. However, based on the secondary legislation and on the initial informal consultations with the Agency, the Agency's interpretation is that such transfer approval will be necessary for cross-border/boundary data transfers to economies outside EU/EEA. This was later confirmed by the Agency's Deputy Director as well, who stated that the Agency's reasoning is that for control purposes they have decided to remain on the firm stance that an approval must be issued for transfer of personal data to third economies and international organisations, having in mind that in practice they have encountered various examples of misuse of personal data in these cross-border/boundary transfers. In relation to this, the Agency has not adopted adequacy decisions yet.

Another example is the consent requirement for processing personal data for direct marketing purposes (**"Direct Marketing Processing"**). The Old Data Protection Law required obtaining consent for each Direct Marketing Processing. However, the Current Data Protection Law prescribes that Direct Marketing Processing which includes profiling to the extent to which it is connected to the direct marketing is allowed only if the previous consent is obtained from the data subject. This provision is drafted in a way that it can be interpreted differently and can suggest that the consent is required only for Direct Marketing Processing which includes profiling. However, the Agency is still on the position that the consent of the data subject is necessary for any Direct Marketing Processing.

The newly adopted bylaws still pose an administrative burden on data controllers, providing that the approval of the Agency is required for processing personal data in many cases (e.g. for transfer of personal data to third economies or international organisations in the prescribed situations, for processing of the data subject's personal identification number when the processing is based on the previous explicit consent by the data subject and a systematic and extensive processing is done under this basis, etc.). The deadline for the Agency to decide on the request for approval was extended to 90 days from receiving the request (compared to the Old Data Protection Law which envisaged a period of 30/60 days). This additionally extends and complicates the procedures and can be detrimental for data controllers and data processors which in many cases need to start processing certain personal data as fast as possible, and such lengthy approval procedure could be detrimental for their business.

Implementation of data protection by design and default and the accountability principle appear to be quite a challenge for data controllers and data processors. Firstly, the Current

Data Protection Law and the adopted bylaws are not entirely clear on what internal documentation must be adopted by each data controller and each data processor and what internal documentation can be adopted/adapted. Secondly, entities must implement various technical and organisational measures from the very creation/further development of their IT system, which can be a very costly matter, and would involve hiring experts from various fields, legal, IT experts, etc., obtaining adequate equipment/software, hiring qualified personnel, training their employees, etc. Small and medium sized enterprises ("**SMEs**") will be most affected by this issue.

Even though the Agency has developed some guidelines and manuals on different topics, they do not encompass all relevant data protection areas and could benefit from guidance on practical implementation. The Deputy Director of the Agency confirmed that they are considering developing guidelines for several topics and will work on them in the coming period.

Many data controllers will likely fulfil the requirements for appointing a DPO. The Current Data Protection Law prescribes several conditions which the DPO must fulfil. The wording of this Law implies that the actual DPO should be a natural person (e.g. must actively use Macedonian language; has a higher education degree; etc.). Accordingly, a legal entity cannot be the actual DPO. It can be argued that in practice the obligations of the DPO can be conducted by legal entities specialised in data protection matters more efficiently, and this limitation of the Current Data Protection Law's wording makes such option impossible. Additionally, the DPO's position should be strengthened in practice.

The Current Data Protection Law envisages that controllers or processors not established in the Republic of North Macedonia should designate a representative in the economy. As far as we are aware, this provision was still not tested in practice. Another right which is not used in practice is the right to data portability.

Furthermore, there is a challenge of implementation of the personal data protection rules and principles by media workers, especially in cases where the freedom of speech is affected.

Low amount of inspection supervision conducted by the Agency contributes to poor implementation of the Current Data Protection Law, while to the best of our knowledge, no misdemeanour procedures were initiated under the Current Data Protection Law. This was the general approach undertaken by the Agency under the Old Data Protection Law as well. As an illustration, according to the 2019 Annual Report of the Agency[23], during 2019 the Agency performed a total of 190 inspection supervisions, out of which 55 were regular, 111 were extraordinary and 18 were control supervisions. Only in 47 cases a breach of the law was determined. Compared to 2018, the number of regular supervisions in 2019 was reduced by 65%, and number of control supervisions by 33%, while the number of extraordinary supervisions increased by 9%.

In 2019, only four misdemeanour procedures were initiated. The Agency's general approach has so far been preventive instead of punitive and directed towards ensuring data protection compliance, due to which data controllers and data processors generally had a perception that an inspection and non-compliance would not have significant implications on them. The Current Data Protection Law imposes fines in the amount of up to 4% of the total annual turnover of the preceding financial year. In comparison, the Old Data Protection Law provided for much lighter penalties ranging up to EUR 2,000 for the breaching entity and up to EUR 600 for the entity's responsible person.

Controllers which are dissatisfied with the decisions of inspectors can submit a lawsuit against the decision to the Administrative Court of the Republic of North Macedonia. In

23 https://dzlp.mk/sites/default/files/u4/godisen_izvestaj_dzlp_2019.pdf

2019, a total of eight administrative disputes were initiated against decisions adopted based on extraordinary supervisions. The disputed decisions refer to: illegal video surveillance in a hotel and a family house, employment relationship in a health institution, publication of a proposal for initiating disciplinary proceedings, processing of a personal identification number in the form of a statement with which they agree/do not agree to transfer the management of the residential building to the competence of the professional manager.

In 2019, a total of 14 judgements were adopted by the Administrative Court and the Higher Administrative Court of the Republic of North Macedonia, out of which 12 judgements refer to administrative disputes initiated prior to 2019. Four lawsuits against the decisions of the inspectors were accepted by the Administrative Court, while six lawsuits were rejected as unfounded and the decisions of the inspectors were confirmed. The Higher Administrative Court, acting upon the appeals against the judgements of the Administrative Court, rejected all four appeals of the controllers. This suggests that a very few supervisions actually end up in court.

In addition to the Agency's general approach, a relevant factor affecting the small number of supervisions is the total number of employees in the Agency which was 23 as of 31 December 2019, which is less than 50% of the actual human resources needed for effective operation of the Agency (a total number of 50 individuals should be employed in the Agency in line with the applicable job systematisation)[24]. Furthermore, in 2019 the Agency was acting without an appointed Director and Deputy Director for a period of six months, which directly influenced the work of the Agency, especially the number of regular inspections performed, opinions issued and training delivered.

The process of implementation of the Current Data Protection Law has been further slowed down by the occurrence spread of Covid-19 in the world and in North Macedonia, which was enacted right at the time of the outbreak. The Agency, as well as other institutions, worked in reduced capacity for several months, and getting in touch with them was very difficult. Generally, the availability of the Agency should improve.

From the aspect of public awareness, general impression is that data subjects are not very familiar with their data protection rights, while data controllers and data processors are not fully aware of their data protection obligations. According to the 2019 Annual Report of the Agency, 60% of the complaints submitted referred to abuse on social media, while many other complaints related to crimes, insults, blackmail and threats, for which the Agency is not competent.

Specifically, during 2019, a total of 216 complaints referring to abuse on social media were submitted to the Agency. The reasons included fake profiles, hacked profiles, publishing someone else's photos, video and audio recording on social media, misuse of personal data while participating in fake prize games on social media, complaints regarding insult, defamation and online blackmail.

The other 40% of the complaints submitted to the Agency in 2019 referred to: processing of personal data through video surveillance in residential buildings and houses, rights of personal data subjects, direct marketing, manner of exercising the right to protection of personal data, processing of personal identification number and/or ID card (copy), the balance between free access to public information and personal data – when and which personal data can be published/publicly available, and which personal data are protected, especially in relation to employee data, etc.

On 29 September 2020, the Agency published a Report on questionnaire assessing the state of personal data processing in local self-government units in North Macedonia[25].

24 2019 Annual Report of the Agency, page 7.

25 https://dzlp.mk/sites/default/files/u4/izvestaj_opstini.pdf

The analysis showed that the municipalities have not established a full data protection system. The questionnaire was submitted to a total of 71 municipalities, of which only 22 municipalities returned a completed questionnaire, which is a devastating statistics given the principle of accountability. The Agency prepared a list of recommendations which the municipalities should implement in order to comply with the Current Data Protection Law.

As part of 2017-2022 Strategy, a SWOT analysis was performed on the current state in the data protection area, which shows the following results:

1. Strengths:
   - Established institutional framework (existence of the Agency);
   - Compliance of the Data Protection Law with EU legislation and international documents;
   - Active training system;
   - Established DPO system;
   - Rulebook on internal and external control;
   - Willingness to keep up with the latest IT technologies;
   - Experienced and dedicated staff of the Agency.
2. Weaknesses:
   - Lack of full harmonisation of special laws with the Data Protection Law and European standards;
   - Limited resources (personnel and funding) of the Agency;
   - Status/support of DPOs within their organisations;
   - Low level of privacy impact and assessment of data security in IT activities/ interconnections;
   - There is still a need to further strengthen the awareness and culture of personal data protection.
3. Opportunities:
   - Use of EU funds/further professional support;
   - Involvement of NGO sector;
   - Opening of the EU accession process;
   - Expanding international cooperation, exchange of experiences and information.
4. Threats:
   - Political crisis, adoption of regulations in urgent procedure;
   - Other policy priorities (security, sectoral, political, etc.) may weaken the impact;
   - Data Protection Law gets out of focus due to critical events/state of emergency (incidents, natural disasters, political or economic crises, etc.);
   - Delay in EU accession.

Considering a general low level of enforcement, it can easily happen that the level of compliance with the data protection requirements imposed by the respective law would be as low as it was with respect to the Old Data Protection Law.

For the sake of avoiding such scenario – avoiding creation of non-compliance environment as the “normal” state of affairs which does not lead to any actual sanctions or damages regardless of the breaches of the law, the following steps should be undertaken as the priority:

1. Inspection supervision of the Current Data Protection Law should be intensified (to the extent possible considering the existing staff restraints faced by the Agency);
2. Offence proceedings should be initiated without exception against data controllers/ processors breaching the law;
3. Public awareness of the data protection importance (in particular when it comes to the rights data subjects have under the Current Data Protection Law) should be further raised (this shall further lead to the more significant reputational risk for data controllers/processors);
4. The fact that the Current Data Protection Law is generally aligned with the GDPR along with the fact that GDPR, due to its extraterritorial effect, may be fully applicable to local data controllers/processors as well, should be emphasised continuously;
5. The legislation should be further liberalised especially in the terms of data transfer and database registration requirements considering that implementation of such requirements is not possible without significant involvement of Agency staff which would, consequently, lead to further reductions of Agency’s capacities in the crucial fields of its activities (such as its inspection supervision activities).

5. CRUCIAL STEPS FOR OVERCOMING THE EXISTING CHALLENGES

To overcome these challenges various steps can and should be taken. These steps should ensure avoiding creation of non-compliance environment as the “normal” state of affairs which does not lead to any actual sanctions or damages regardless of the breaches of the law, as well as increase the perception about the importance of data protection.

As a priority, the Agency and other stakeholders should work on adopting the remaining bylaws and achieving harmonisation of the sector legislation with the Current Data Protection Law.

In the legislative area, the Agency should focus on adopting additional bylaws to further regulate matters prescribed by the Current Data Protection Law, such as:

1. Procedures for securing standardised icons and identifying the information to be represented as standardised icons;
2. Rulebook on keeping the registry of approved codes of conduct;
3. Standards and norms for accreditation of a body for monitoring the compliance of the codes of conduct;
4. Certification standards and norms for personal data protection and accreditation of certification bodies;
5. Rulebook on keeping the registry of all certification mechanisms, as well as data protection seals and marks; etc.

The Agency should keep a registry of the approved codes of conduct, certification mechanisms and data protection seals and marks, and make them publicly accessible. This would provide transparency and valuable information to data controllers, data processors and data subjects, and would promote and encourage entities to implement these tools/ mechanisms.

The Deputy Director of the Agency informed us that the new internal acts under the Current Data Protection Law are being finalised and will be published soon. The Agency is also

preparing a DPIA methodology and guidelines on the issue of evaluating the legitimate interest for processing personal data as a legal basis for the respective processing.

The Ministry of Justice of the Republic of North Macedonia and other competent authorities should accelerate the process of transposing the Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02016L0680-20160504) on the protection of natural persons with regard to the processing of personal data by competent authorities for the purpose of law enforcement. This should provide a regulatory framework for personal data processing by the police and other law-enforcement authorities. The Agency Deputy Director informed us that the law which should transpose this directive was already prepared and delivered to the relevant ministries, and that he expects it to be adopted by the end of the year. Also, in the near future the Agency and the Ministry of Interior are to sign a Memorandum of Cooperation which will set the framework for future projects in which experts from both institutions will cooperate[26].

When it comes to harmonisation of sector legislation with the Current Data Protection Law, a study should be conducted in order to design a best possible approach for harmonisation. The Agency should be consulted throughout the process of harmonisation and should issue opinions on the draft laws and bylaws as regards their level of harmonisation with the Current Data Protection Law prior to the draft laws and bylaws being accepted and proposed as such to the relevant institutions. For example, in 2019, the Agency issued expert opinions on the following laws/regulations and to the following public institutions:

1. Law on Central Population Register - Ministry of Information Society and Administration of the Republic of North Macedonia;
2. Law on Electronic Management and Electronic Services - Ministry of Information Society and Administration of the Republic of North Macedonia;
3. Law on Electronic Documents, Electronic Identification and Confidential Services - Ministry of Information Society and Administration of the Republic of North Macedonia;
4. Law on National Security Agency - Ministry of Interior of the Republic of North Macedonia;
5. Draft Law Amending the Law on National Bank of the Republic of North Macedonia – Ministry of Finance of the Republic of North Macedonia;
6. Draft Law on Prevention and Protection from Violence against Women and Domestic Violence - Ministry of Labour and Social Policy of the Republic of North Macedonia;
7. Decree on maintaining the Integrated Database on Foreigners, including data on asylum, migration and visas, and on mutual relations of the competent authorities in the process of maintaining the Database - Ministry of Interior of the Republic of North Macedonia;
8. Decree on ensuring confidentiality, protection and security of data contained in the Integrated Database on Foreigners including data on asylum, migration and visas - Ministry of Interior of the Republic of North Macedonia;
9. Law on Management of Case Flows in Courts - Ministry of Justice of the Republic of North Macedonia;
10. Rulebook on keeping a register of members of the Chamber of Health Workers with Secondary and Tertiary Education of the Republic of North Macedonia – Chamber of Health Professionals with Secondary and Tertiary Education of the Republic of North Macedonia;
11. Rulebook on amending the Rulebook on the form and content of the request and the instruction on filling in the request for authorisation of the persons/ trainers to deliver training in general professional ability to train drivers, in professional knowledge and competence related to the railway vehicle and professional knowledge and competence regarding the railway infrastructure, the form and content of the authorisation and the form and content of the Register of issued authorisations - Ministry of Transport and Communications of the Republic of North Macedonia;
12. Rulebook on amending and supplementing the Rulebook on ensuring security and integrity of the public electronic communication networks and services and activities operators should undertake in case of violation of the personal data security - Agency for Electronic Communications of the Republic of North Macedonia;
13. Rulebook on supplementing the Rulebook on the form and content of the knowledge, skills and competencies certificate issued interns, and description and duration of internship - Ministry of Labour and Social Policy of the Republic of North Macedonia.

For comparison, according to the 2019 Annual Report of the Assembly of the Republic of North Macedonia, total number of laws which were adopted in 2019 was 196, while the number of adopted decisions was 105. This strongly suggests that the involvement of the Agency in the legislative process should be intensified.

The relevant stakeholders should pursue achieving full compliance with the GDPR and amending the Current Data Protection Law and its bylaws (e.g. to exclude the registration in the High-Risk Records, to enable appointment of a legal entity as a DPO, to clarify that the consent of the data subject for each data processing for direct marketing purposes is not necessary if different legal ground applies to the processing, to remove the requirement to request the Agency's approval for transfer of personal data to a third economy for which an adequacy decision was adopted by the Agency, etc.). The amendments should also introduce a shorter period of time for the Agency to issue approvals. These amendments would reduce the administrative burden on the Agency and on data controllers too and would enable reallocation of the capacity of the Agency's personnel to other matters such as supervision.

The Agency should also adopt standard contractual clauses between data controllers and data processors, and standard contractual clauses between data transferors and data recipients in case of cross-border/boundary transfer of personal data and adequacy decisions for third economies.

Experts should be involved in the process of adoption of the abovementioned acts and documents, especially GDPR experts who will ensure that the essence of the GDPR is transposed into these documents. It should be constantly emphasised that the GDPR itself may be fully applicable to local data controllers/processors due to its extraterritorial effect. Establishing an active cooperation with other data protection authorities, especially in the European Union, would be beneficial. This can also be achieved by the Agency taking active participation in international events and forums, as well as participating in and taking initiatives for joint activities with data protection authorities from other economies.

The Agency and other relevant bodies should work on obtaining an adequacy decision from the European Commission that the Republic of North Macedonia has an adequate level of data protection.

In addition to the above, it would be constructive the Agency develops additional documents and mechanisms to make the implementation of the Current Data Protection Law easier

26 https://www.dzlp.mk/mk/content/%D0%B4%D0%B8%D1%80%D0%B5%D0%BA%D1%82%D0%BE%D1%80%D0%BE%D1%82-%D0%BD%D0%B0-%D0%B0%D0%B3%D0%B5%D0%BD%D1%86%D0%B8%D1%98%D0%B0%D1%82%D0%B0-%D0%B7%D0%B0-%D0%B7%D0%B0%D1%88%D1%82%D0%B8%D1%82%D0%B0-%D0%BD%D0%B0-%D0%BB%D0%B8%D1%87%D0%BD%D0%B8%D1%82%D0%B5-%D0%BF%D0%BE%D0%B4%D0%B0%D1%82%D0%BE%D1%86%D0%B8-%D0%B3-%D0%B8%D0%BC%D0%B5%D1%80-%D0%B0%D0%BB%D0%B8%D1%83-%D0%BE%D1%81%D1%82%D0%B2%D0%B0%D1%80%D0%B8-%D1%80%D0%B0%D0%B1%D0%BE%D1%82%D0%BD%D0%B8

and more understandable for data controllers, data processors, data subjects and third parties. Particularly, the Agency can develop guidelines on different topics, good practice documents, various templates, handbooks, check lists, etc.

It would be very beneficial that manuals and guidelines are developed to cover matters which are not explicitly regulated (for example, which internal data protection acts must be adopted by data controllers and data processors, guidance on data controllers that have an obligation to appoint a DPO, etc.) as well as matters which inspections have so far determined to be most frequently breached by data controllers and data processors (for example, according to the 2019 Annual Report of the Agency, the top three violations of the Old Data Protection Law include: (i) 105 violations – lack of technical and organisational measures for secrecy and protection of personal data processing; (ii) 63 violations – lack of personal data processing agreement between the data controller and the data processor; and (iii) 41 violations – non-exercise of the data subject rights to access, correction and deletion of their personal data).

The Agency can issue guidelines on how to apply the Current Data Protection Law to specific areas, such as technological developments, health related data processing at times of pandemics, blockchain and artificial intelligence, etc. When it comes to the data portability right and the lack of its implementation in practice, a project can be introduced and implemented so that innovative solutions are designed and developed which would enable provision of data in a machine-readable format and allow data subjects to switch between service providers (for example, mobile applications for data management and transfer, tools for providing and withdrawing consent, tools for requesting access to the personal information, etc.).

A project aimed at assisting the implementation of the Current Data Protection Law by SMEs, charitable organisations and associations could be implemented, where project beneficiaries would be provided with templates and other practical tools, as well as training and grants for data protection compliance.

Having in mind the increased number of IT companies in North Macedonia and their fast expansion, as well as the vast amount of personal data which they could encounter in their regular business, the Agency should focus on IT companies and their compliance with the Current Data Protection Law.

Additionally, the Agency should be focused on data protection compliance of sports betting companies, casinos and similar companies given that in 2019 15% of the extraordinary supervisions conducted by the Agency were related to misuse of personal data by sports betting companies. The cases elaborated in the 2019 Annual Report of the Agency referred to citizens being surprised to find out that winnings from games of chance were paid on their behalf. During the extraordinary supervisions, the Agency determined that the sports betting companies: (i) did not have internal procedures for checking the quality of their client's data; (ii) the employees of the sports betting companies were not informed about personal data protection; and (iii) the sports betting companies did not keep records of each authorised access (logs) when processing personal data through the applicable software and during the direct access to the databases. The Association of Sports Betting Companies of North Macedonia took an initiative to find a permanent solution to the verification and updating of players data with the competent institutions. However, to this end it will be necessary to adopt amendments to certain laws.

The Agency should work on raising awareness about personal data protection (for example, media workers must be trained on how to make a balance between the protection of personal data with freedom of expression and information) and obligations of data controllers and data processors, and on designing mechanisms and tools which would enable greater availability and access for concerned private entities.

The Agency can conduct a study on the level of data protection awareness of the general public. This would offer a clear overview of the current situation, according to which the necessary steps for increasing awareness can be tailored. The Agency should consider publishing articles and other information through a profile on Facebook, Twitter and other communication and social networking platforms used by the general public, since such communication steps would reach many concerned individuals.

Although the webpage of the Agency contains extensive information which is in line with the Old Data Protection Law, the information needs to be updated to reflect the Current Data Protection Law. The Agency can publish educational videos, podcasts, articles, and general information on its webpage. It can also publish magazine articles, newsletters and write press releases.

Awareness of the population can be raised through data protection training, which should start even in schools, for which purpose the Agency could cooperate with the Ministry of Education and Science of North Macedonia. Seminars and webinars on different data protection topics can be held, inviting experts in this field. Also, the Agency should ensure that every DPO has undertaken data protection training and should undertake steps to strengthen the position of DPOs, such as further develop the DPO network and encourage its use and the use of all available tools developed by the Agency and available to DPOs. The Agency can encourage establishing DPO association.

Agency employees should be trained and educated on how to respond to questions from interested entities and natural persons regarding the implementation of the Current Data Protection Law, especially to provide concrete answers and not merely cite laws, and give particular and practical examples. Agency employee's understandings on the administrative procedures and the general idea of the GDPR which should be transposed in North Macedonia should be improved and no additional requirements should be introduced in their daily work.

Training should include theoretical and practical classes.

A platform for questions and answers could be developed where anyone can submit a question to the Agency, which would then respond to the question and the questions and answers on each topic would be saved on the platform where any interested person could access them and search through the data protection questions most frequently posed. This tool would significantly help the implementation of the Current Data Protection Law as it would save time and resources, as well as free the Agency from receiving constant questions referring to the same subject matter. A similar tool is already used by the Public Revenue Office of the Republic of North Macedonia available at http://kontaktcentar.ujp.gov.mk:8090/ISKnowledgeBaseExternal/Search/Index and it has proved to be a valuable asset in practice.

The independent status of the Agency should be strengthened, which can be achieved by securing the necessary budgetary funds (especially through own funds generated by delivering training, issuing certificates, etc.). Also, investments in the employees in the Agency should be made in terms of salary increase, and professional advancement and employee training. The Agency can cooperate with various experts in the field and seek aid when necessary.

The progress of implementation of the relevant strategies should be measured, especially of the 2017-2022 Strategy and the Communication Strategy. The Agency's management should check the status quarterly and annually and define potential corrective measures. It would be prudent to present the annual results and discuss them in a staff meeting. If the desired results are not achieved the suggested corrective measures include: focusing additional attention of the management and/or providing resources if the priority of the assignment is still high and the actions which would help the assignment are still relevant,

revising action plan/the assignment if the priority of the assignment is still high and the undertaken actions do not result in realization of the assignment; reviewing the relevance of the assignment.

Furthermore, the important role of the Agency can be strengthened especially in the eyes of private entities and natural persons, if the public sector sets an example of trust, compliance with the measures, observations, recommendations, opinions and instructions of the Agency and recognition of its independent role in North Macedonia.

Training and data protection education sessions should be held for public officials and employees in other public institutions in order to raise their awareness and approach to data protection matters. For example, the most recent case of non-compliance with the Current Data Protection Law which was publicised was the violation made by the State Election Commission during the 2020 extraordinary parliamentary elections. After holding the early parliamentary elections, an incident occurred where the website/web services of the State Election Commission were not available for a certain period. The Agency conducted supervision[27] and determined several violations such as: the State Election Commission did not apply appropriate technical and organisational measures, it did not test the software system of the data processor, it did not perform a data impact assessment, it breached the provisions for cross-border/boundary transfer of personal data, it did not notify the Agency on the personal data breach. The State Election Commission has a vast amount of personal data of voters, and as such has various data protection obligations. However, the recent case shows that the data protection matters were not taken seriously by an institution processing vast amount of personal data. Such situations must be avoided in the future by raising data protection awareness of other public institutions and performing regular supervision.

Another recent example of non-compliance with the Current Data Protection Law by public institutions resulted from the hacker attack on the websites of the Ministry of Education and Science of the Republic of North Macedonia and the Ministry of Health of the Republic of North Macedonia in July 2020. The Agency published on its website that it initiated supervision[28] over the legality of the activities undertaken in the processing of personal data and their protection by the Ministry of Education and Science and the Ministry of Health because neither of the ministries notified the Agency of the personal data breach as prescribed by the Current Data Protection Law. However, there is still no available information as to the results of this supervision.

It would be beneficial if the Agency would frequently publish the steps that it is undertaking, relevant investigations and inspections which are taking place, the results of these investigations and inspections. Efforts should be made to ensure impartial and independent work of the Agency through distance supervision and electronic means, as much as possible.

The Agency's Director and Deputy Director, as well as other Agency representatives could intensify their media appearance and discuss different topics, especially hot topics which would draw the attention of general public, such as abuse of personal data online, fake profiles, hacking accounts, video surveillance, etc. The Agency can have open days to promote its work.

We believe that one of the most efficient steps would be for the Agency to conduct more supervisions and initiate misdemeanour procedures if determined that the Current Data

27 https://dzlp.mk/mk/content/%D0%BD%D0%B0%D0%BE%D0%B4%D0%B8-%D0%BE%D0%B4-%D1%81%D0%BF%D1%80%D0%BE%D0%B2%D0%B5%D0%B4%D0%B5%D0%BD%D0%B0%D1%82%D0%B0-%D1%81%D1%83%D0%BF%D0%B5%D1%80%D0%B2%D0%B8%D0%B7%D0%B8%D1%98%D0%B0-%D0%B2%D0%BE-%D0%B4%D0%B8%D0%BA

28 https://dzlp.mk/mk/content/%D0%B0%D0%B7%D0%BB%D0%BF-%D1%81%D0%BF%D1%80%D0%BE%D0%B2%D0%B5%D0%B4%D1%83%D0%B2%D0%B0-%D1%81%D1%83%D0%BF%D0%B5%D1%80%D0%B2%D0%B8%D0%B7%D0%B8%D1%98%D0%B0-%D0%B2%D0%BE-%D0%BC%D0%BE%D0%BD-%D0%B8-%D0%BC%D0%B7-0

Protection Law was violated, without exceptions. This, however, does not exclude the provision of advice and support for achieving compliance which the Agency should provide to data controllers and data processors. The Deputy Director of the Agency informed us that the Agency had already started conducting online supervisions. He also informed us that the Agency's approach to supervision will change compared to its approach to inspections during the validity period of the Old Data Protection Law. The Agency will be tolerant until the expiry of the compliance period, unless there is an obvious and intentional or reckless privacy breach. In any case, the Agency will move forward with issuing fines for committed misdemeanours. In this sense, it is important that the responsible inspectors in the Agency who will be issuing the fines undertake appropriate training covering procedural and substantive matters. The procedural training should ensure that the issued fine is well based and does not breach any procedural rule which could render it invalid, while substantive training should ensure that the responsible Agency staff applies the relevant provisions of the Current Data Protection Law and other applicable laws when issuing fines.

The Deputy Director of the Agency takes the view that supervision will be conducted differently in the period to come compared to the inspection under the Old Data Protection Law. Previously, the Agency conducted inspections by providing a control list to data controllers and data processors requesting to be provided with all documents and information on the list. On the other hand, the supervision under the Current Data Protection Law will be conducted under the principle of accountability, where data controllers and data processors will be asked to prove that they compliant with the Current Data Protection Law, without the Agency requiring to be provided with specific documents and information and all this will be based on the risk analysis which should be performed.

On the other hand, data controllers should themselves invest in data protection compliance measures and undertake actions in order to achieve compliance with the Current Data Protection Law as soon as possible, even though they have little less than a year left to achieve full compliance (until 24 August 2021). Data controllers could perform an internal due diligence on their established data protection system and especially: identify all personal databases and risks from processing the identified personal data, analyse the status of the appointed DPO and the DPO's independence, assess technical and organisational measures that need to be updated/amended/enhanced, re-evaluate their data processors and review the agreements with the data processors, establish or re-assess the system for data protection training of their employees, review the cross-border/boundary transfers of personal data and their compliance with the Current Data Protection Law, perform internal and external data protection controls, etc. Data controllers should prepare an action plan on their compliance with the Current Data Protection Law.

The outbreak and spread of Covid-19 in North Macedonia had a big impact on data protection. Due to the fast spread and the easy transmission of the virus, it became one of the biggest threats to human life and health, as well as businesses and the economy in 2020. This especially impacted the business processes of large companies employing many employees, as some of them had to cease their work, while others even closed down their companies. Realising that the Coronavirus will be here for some time and that employers need to adapt to the new situation, they became creative in ensuring that the number of employees that will get infected with the virus is brought to a minimum. In addition to other protective measures which employers undertake, they started using advanced technology, some of which raises data protection concerns, as well as large-scale data processing. Furthermore, revealing personal data of employees which are infected with Covid-19 is also questionable. Many employers decided to introduce work from home, which in many cases lead to monitoring of the employees, e.g. through video. Data protection concerns caused by the coronavirus spread in other areas, such as education, media, health system, etc., while during the declared state of emergency in 2020, numerous decrees with a force of law were adopted by the Government of the Republic of North Macedonia which suggested

undertaking actions which infringed data protection rights of data subjects. Even though it is undisputed that the right to human life and health prevails, it is of crucial importance to keep the data protection rights to the highest level possible. As it is evident that the Coronavirus will not disappear easily nor very soon, it is very important that the Agency devotes its attention to achieving a high standard of data protection during the pandemic. This can be done by preparing guidelines on how to deal with the pandemic from a data protection perspective (the Agency already published a text on this issue[29]), advising government bodies and data controllers directly, preparing and publishing opinions on whether certain technologies and monitoring fulfil the data protection requirements and performing supervisions.

To conclude, it is of outmost importance that steps are undertaken to overcome the challenges described above, starting from the adoption of remaining bylaws and the law transposing the EU police directive, harmonisation of the sector legislation and increasing the functional independence of the Agency. The Agency can then focus on performing supervisions and training its staff further, as well as preparing guidelines for data controllers and processors to help them achieve compliance with the Current Data Protection Law. Finally, the Agency should work on increasing public awareness as well as awareness in the public and private sector about personal data protection and data privacy matters.

29 https://dzlp.mk/mk/content/%D0%B7%D0%B0%D1%88%D1%82%D0%B8%D1%82%D0%B0%D1%82%D0%B0-%D0%BD%D0%B0-%D0%BB%D0%B8%D1%87%D0%BD%D0%B8%D1%82%D0%B5-%D0%BF%D0%BE%D0%B4%D0%B0%D1%82%D0%BE%D1%86%D0%B8-%D0%B8-%D0%BA%D0%BE%D1%80%D0%BE%D0%BD%D0%B0%D0%B2%D0%B8%D1%80%D1%83%D1%81%D0%BE%D1%82#overlay-context=

CHAPTER VI. SERBIA

1. CURRENT STATUS

The main law governing data protection and privacy in Serbia is the Law on Protection of Personal Data (Official Gazette of the Republic of Serbia, no. 87/2018) (“**Current Data Protection Law**”).

The Current Data Protection Law superseded the Law on Protection of Personal Data which originates from 2008 (“**Old Data Protection Law**”) and which was applicable as of 1 January 2009, therefore for more than a decade before the Current Data Protection Law became applicable.

The Old Data Protection Law deficiencies were detected in the course of its application and significant improvements were needed. The most important deficiencies existed in the field of data transfer regime, sensitive data (i.e. special categories of personal data) and legal grounds for legitimate processing of personal data.

Data transfer regime prescribed by the Old Data Protection Law was an issue because, unlike the current data transfer regime envisaged by the GDPR and the Current Data Protection Law, it was rather blocking than enabling data flow which, in contemporary multi-jurisdictional business environment, is a considerable obstacle to the day-to-day operations.

Specifically, the Old Data Protection Law prescribed only one scenario under which a transfer of personal data from Serbia to vast majority of non-European economies can be performed legitimately without obtaining prior approval of the Serbian data protection authority for a particular transfer. This is the scenario under which data is to be transferred to an economy which is a member of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. In any other case when personal data should be transferred to any economy which has not signed and ratified the Convention (e.g. to the USA), the only mechanism for ensuring that a data transfer out of Serbia is performed in line with the Serbian law was to obtain prior approval from the Serbian data protection authority. However, in practice, the procedure for obtaining the respective approval (when such approval, in line with the above, was needed) often lasted a long period of time (measured in months) and the requirements were very strict. As a result, many legal entities did not even apply for transfer approvals (although they should have done so considering economy(ies) to which they have transferred data) and, consequently, level of compliance with the Old Data Protection Law was very low.

The Current Data Protection Law changed (or at least intends to change) this by introducing the whole set of mechanisms based on which a legitimate transfer of data out of Serbia is possible (with or without prior data transfer approval), as further elaborated in Section 2 (item 8) below.

Further, when it comes to sensitive data (special categories of personal data), perhaps the biggest concern of the Serbian data protection authority in the course of the Old Data Protection Law application was the issue of the adequate protection of the respective personal data.

More precisely, the Old Data Protection Law prescribes that any processing of sensitive data has to be specially marked and protected by security measures (in a sense that such measures should be stricter that those necessary to apply when “regular” personal data is processed). It is also prescribed that such measures are determined by the Serbian Government upon obtaining prior opinion of the Serbian data protection authority. However, such measures have never been specified (i.e. the Government has never adopted any

regulation/rulebook governing the respective issue) and, consequently, the respective statutory obligation of undertaking special security measures when processing sensitive data remained relevant in theory only.

The Current Data Protection Law has fully aligned the Serbian data protection law with the GDPR in the field of special categories of personal data by introducing the same definition/ scope of the respective data (broader than under the Old Data Protection Law) and the same regime of the respective data processing (i.e. regime under which any processing of such data is forbidden subject to certain exceptions explicitly governed by the law, such as, for example, a data subject's consent or necessity of a particular processing for fulfilment of an important public interest determined by a law, etc.). Further details on the processing of special categories of data under the Current Data Protection Law are provided in Section 2 (item 4) below.

In addition to the above, one of the biggest concerns with applicability of the rules envisaged by the Old Data Protection Law was the issue of legal grounds for legitimate data processing. This law did introduce consent (a prior informed consent) of a data subject and a few other legal grounds, but the manner in which such other legal grounds were formulated made them inapplicable, fully or to a significant extent, in practice, or at least led to significant legal uncertainty (due to uncertainty whether a particular statutory ground would indeed be considered as applicable/adequate for a particular processing). For example, it was, amongst other, prescribed that a data processing was allowed without a data subject's consent "in other cases prescribed by this law, for the purpose of fulfilment of a prevailing justified interest of a data subject, data controller or data user". This legal ground is actually a "variation" of a legal ground of legitimate interest as prescribed by both the Current Data Protection Law and GDPR; however the issue was that the Old Data Protection Law actually did not prescribe any particular cases to which it is referred in the aforementioned provision on the respective legal ground.

Finally, it was necessary, not only with respect to the above issues, but in general as well, to align the Serbian data protection legislation with the new EU data protection regulation – with GDPR.

The adoption of the Current Data Protection Law was aimed to serve this purpose. The Law entered into force on 21 November 2018. Upon expiry of a nine-month transition period, it became applicable on 21 August 2019. This is, accordingly, the first year of its application.

The Current Data Protection Law represents a copy of the GDPR in its biggest part. Nevertheless, certain differences do exist, whereas the most obvious one is that the penal policy envisaged by the Current Data Protection Law is significantly milder than the one governed by the GDPR.

Specifically, the highest possible fine under the Current Data Protection Law is the fine of RSD 2 million (approx. EUR 17,000) for a legal entity and RSD 150,000 (approx. EUR 1,300) for a legal entity's representative or a natural person.

Other than this, it should also be noted that the Current Data Protection Law does not envisage any of the recitals introduced by the GDPR (it contains 173 recitals) and, thus, lacks the explanations as a very important tool for its full understanding and adequate application.

Apart from that, although the Current Data Protection Law introduced many important improvements and novelties, it still did not govern certain issues which have not been governed by the Old Data Protection Law either, such as the rules on video surveillance and processing of biometric data.

In this regard, it should be mentioned that video surveillance, including its data processing perspective, is governed by a dedicated law – Private Security Law originating from 2013.

Under this law, data collected in the performance of private security activities can be used solely for the purpose for which they were collected and cannot be provided to third parties or announced publicly, unless agreed or prescribed differently. The confidentiality obligation is also envisaged as the obligation of all legal entities and entrepreneurs involved in the private security business, as well as of all individuals (security staff) involved in performance of the respective activities. When it comes to the retention term, users of private security services are obliged to keep the respective video-recordings for at least 30 days and to provide them, upon request, to an authorised police officer.

On the other hand, when it comes to biometric data, the Current Data Protection Law does envisage their definition and that they belong to so-called special categories of personal data, but does not prescribe any specific rules on their processing. Such rules are not envisaged by any other law either.

The overview of the most important rules governed by the Current Data Protection Law, compared with the relevant GDPR rules, follows in Section 2 of this Chapter VI.

The relevant secondary legislation will also be covered by the respective overview. This is the secondary legislation which was adopted upon adoption of the Current Data Protection Law, in the course of 2019 and 2020, either by the data protection authority or by the Serbian Government.

The authority competent for data protection matters in Serbia is the Commissioner for Information of Public Importance and Protection of Personal Data ("**Commissioner**"). The Commissioner is seated in Belgrade and its official website is www.poverenik.rs

The Commissioner was established by the Old Data Protection Law as the authority with the exclusive competence both in the field of protection of personal data and in the field of so-called information of public importance – implementation of the right of the public to know/ have access to the information held by public authorities which it has a justified interest to know. This is the reason full name of the Commissioner includes both information of public importance and protection of personal data, as identified above.

Prior to its establishment, there was no such authority in Serbia. At the moment of adoption of the Current Data Protection Law, it has already gained more than a decade of experience in the field of data protection.

Nevertheless, there are still some challenges in the Commissioner's work which remained even after the adoption of the Current Data Protection Law (such as insufficiency of staff particularly in the field of inspection supervision or the fact that some important issues, such as for example video surveillance related data processing, remained out of the scope governed by the Current Data Protection Law).

Further information on the Commissioner, its competences and challenges in its work in the field of personal data protection is provided in Section 3 below.

2. ASSESSMENT OF THE LEVEL OF COMPLIANCE OF THE DATA PROTECTION LAW AND RELEVANT SECONDARY LEGISLATION WITH GDPR

As noted above, the Current Data Protection Law is the copy of the GDPR in its biggest part. Therefore, the rules introduced by the respective law are generally aligned with the GDPR, subject to certain exceptions (the aforementioned lack of the stringent penal policy envisaged by the GDPR).

This overview contains summary of the most important rules and areas governed by the Current Data Protection Law, as well as the identification of the most important secondary

legislation and matters prescribed by such legislation, as follows: (1) general data processing requirements, (2) obligations and responsibilities of data controllers and data processors, (3) data protection officers and representatives of foreign entities, (4) special categories of personal data, (5) rights of data subjects, (6) records of processing activities, (7) data breach related notifications and data protection impact assessment, (8) data transfer, (9) penal policy, and (10) relevant secondary legislation.

1. GENERAL DATA PROCESSING REQUIREMENTS

Under the Current Data Protection Law, all personal data, regardless of their type, category of data subjects and scope of a particular processing, should be processed in line with certain processing principles explicitly governed by the respective law, as follows:

1. Personal data should be processed for specified, explicit, justified and legitimate purposes;
2. Processing should be carried out lawfully, fairly and transparently in relation to the data subjects;
3. Processing should be limited to data which is necessary for fulfilment of the processing's legitimate purpose(s);
4. Processed data should be accurate and, where necessary, kept up to date;
5. Processed data should not be retained (in the form which enables identification of a natural person) longer than necessary for the purpose(s) for which they are processed, and
6. Processing should be performed in a manner that ensures appropriate security of the processed data.

The above principles are fully aligned with those envisaged by the GDPR (Article 5).

Also, the same as under the GDPR, the requirement of carrying out the data processing lawfully means that, amongst other, it should be based on adequate legal grounds.

Such legal ground is either a data subject's consent (relating to specified, explicit and legitimate purpose(s)) or one of the remaining grounds explicitly prescribed by the Current Data Protection Law. Specifically, these grounds include:

1. Necessity of a particular processing for the performance of a contract to which a data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
2. Necessity for compliance with a legal obligation to which the data controller is subject;
3. Necessity for the protection of the vital interests of the data subject or of another natural person;
4. Necessity for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller, and
5. Necessity to serve 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 ("**Statutory Grounds**").

It can be clearly seen that each of the Statutory Grounds includes necessity of a particular data processing to achieve a specific legitimate purpose(s).

The legal grounds (consent of data subjects and the Statutory Grounds) envisaged by the Current Data Protection Law correspond to the data processing legal grounds envisaged by the GDPR (Article 6).

Moreover, all data processing requirements identified above are fully aligned with the data processing principles envisaged by the GDPR (Article 5).

2. OBLIGATIONS AND RESPONSIBILITY OF DATA CONTROLLERS AND DATA PROCESSORS

Data controllers and data processors are obliged to perform data processing in compliance with all the data processing principles described above. Data controllers should also be able to demonstrate the respective compliance (accountability).

This should be done by implementing appropriate technical, organisational and human resources measures, whereas the nature, scope, context and purposes of the particular processing, as well as the risks of varying likelihood and severity to the rights and freedoms of natural persons, should be taken into consideration. The measures should ensure adequate protection of the processed data including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. The rights of data subjects should be duly protected.

The measures should be reviewed and updated where necessary and, if proportionate in relation to processing activities, they should also include the implementation of appropriate data protection policies.

The same as the GDPR, the Current Data Protection Law does not prescribe the exhaustive list of the respective measures, but solely provides some examples (such as pseudonymisation and encryption) and describes, in general, their purpose and circumstances to be taken into consideration when deciding on their implementation.

When it comes to the relationship between a data controller and a data processor, a written data processing agreement of the prescribed content should be entered into between them.

This agreement should govern relevant characteristics of a particular processing (such as the nature and purpose of the processing, its subject matter and duration, type(s) of the processed data and category(ies) of data subjects) and mutual rights and obligations of the parties (e.g. obligation of a data processor to process the data only according to the controller's documented instructions, to ensure that the persons authorised to process personal data are obliged to keep the data confidentiality, to return to the data controller or to delete all processed data, including all copies, upon termination of the processing activities envisaged by a data processing agreement unless the obligation of retaining the respective data is prescribed by a law, etc.).

Further, a data controller should only engage a data processor which provides sufficient guarantees that the appropriate measures shall be undertaken in such a way that the processing shall meet statutory requirements and that the protection of the data subject rights shall be ensured.

It is also explicitly envisaged that a data processor should not engage another processor (i.e. sub-processor) without prior written authorisation, general or specific, of the data controller. If a sub-processor in engaged and if it fails to fulfil its data protection obligations, the initial data processor remains fully liable to the data controller for the performance of that sub-processor's obligations.

It should also be emphasised that should a data processor breach provisions of the Current Data Protection Law by determining the purpose and manner of a particular data processing (as their determination is to made solely by a data controller), such data processor shall be regarded as the data controller for that particular processing.

Further obligations of data controllers and/or data processors are described in item 3 and items 5-8 in this Section 2.

3. DATA PROTECTION OFFICERS AND REPRESENTATIVES OF FOREIGN ENTITIES

Under the Current Data Protection Law, the same as under the GDPR (Articles 37 – 39), data controllers and data processors are obliged to appoint a data protection officer ("**DPO**") in certain cases. These are the following:

1. Processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
2. Core activities of the data controller/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, and
3. Core activities of the data controller/processor consist of processing on a large scale of so-called special categories of data and personal data relating to criminal convictions and offences.

Accordingly, the DPO appointment is obligatory only in 3 aforementioned cases – in all other cases its appointment is fully voluntary.

Only a natural person can be appointed as the DPO. Such natural person can either be an employee of a data controller/processor or an externally/contractually engaged person, whereas legal entities which can be regarded as part of the same group of business subjects can have one joint DPO (under condition that he/she would be equally available to each member of the respective group).

In any case, if the DPO is appointed (and, as already mentioned above, such appointment is obligatory only in 3 above-stated cases, it is voluntary in all other cases), the DPO's contact details should be published and communicated to the Commissioner.

It is also prescribed that the DPO should be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks envisaged by the Current Data Protection Law. Specifically, these are the following:

1. To inform and advise the data controller/processor and the employees who carry out processing of their obligations pursuant to the Current Data Protection Law;
2. To monitor compliance with the respective law, other laws and with internal rules of the data controller/processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
3. To provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to the relevant provision of the Current Data Protection Law;
4. To cooperate with the Commissioner, to act as the contact point for the Commissioner and consult with the Commissioner on issues relating to processing, including the prior consultation regarding the data protection impact assessment.

The DPO should, when performing his/her above-stated obligations, have due regard to the risk associated with processing operations, considering the nature, scope, context and purposes of processing. The DPO should also be bound by secrecy/confidentiality concerning the data obtained by performing the above tasks.

It is further prescribed that the data controller/processor which appointed the DPO shall ensure that the DPO is involved, properly and in a timely manner, in all issues which relate to the protection of personal data. The data controller/processor shall also support the DPO in performing the aforementioned tasks by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his/her expert knowledge.

The data controller/processor is obliged to ensure independency of the DPO when exercising the above tasks. The DPO shall not be dismissed or penalised by the data controller/processor for performing his/her tasks. He/she shall report to the data controller's/processor's manager directly. The DPO may, in addition to the above tasks, fulfil other tasks and duties and the data controller/processor shall ensure that any such tasks and duties do not result in a conflict of interests.

When it comes to the relationship between the DPA and data subjects, it is prescribed that data subjects may contact the DPO with regard to all issues related to processing of their personal data and to the exercise of their rights under the Current Data Protection Law.

Furthermore, the same as the GDPR, the Current Data Protection Law introduces, besides the position of the DPO, position of the representative (for data protection matters) of foreign entities to which the respective law is applicable.

Specifically, when the Current Data Protection Law is applicable to foreign data controllers/processors (so-called extraterritorial effect of the law), such foreign entities are obliged to appoint their representative for the territory of Serbia. Unlike the DPO who has to be a natural person, this representative can be either a natural person or a legal entity. In any case, it has to be available as the respective foreign entity's contact point in Serbia to both the Commissioner and local data subjects.

The cases when such extraterritorial effect exists – when foreign data controllers/processors are obliged to appoint their representatives in Serbia are the cases, subject to certain exceptions, when their processing activities are related to:

1. Offering of goods or services to a data subject at the territory of Serbia, irrespective of whether a payment of the data subject is required; or
2. Monitoring of the data subject's behaviour as far as his/her behaviour takes place in Serbia.

The rules envisaged by the Current Data Protection Law with regard to both DPOs and representatives are aligned, subject to certain terminology differences (when it comes to the rules on representatives, i.e. on extraterritorial effect of the law), with the GDPR (Article 3, Article 27 and Articles 37 – 39).

4. SPECIAL CATEGORIES OF PERSONAL DATA

The definition and further rules on processing of these personal data, as prescribed by the Current Data Protection Law, correspond to the respective GDPR rules.

Specifically, special categories of personal data include data revealing racial or ethnic origin, political opinion, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health and data concerning a natural person's sex life or sexual orientation.

In comparison to the Old Data Protection Law (which recognised so-called particularly sensitive data), biometric and genetic data are completely new types of personal data which were not governed by the Old Data Protection Law at all.

In this regard, it should also be noted that, unlike the Old Data Protection Law which governed that data relating to criminal convictions are also amongst special categories of personal data, the Current Data Protection Law does not define them as such. More precisely, the Current Data Protection Law follows the rules on data relating to criminal convictions and offences as such rules are envisaged by the GDPR (Article 10). This means that, under the Current Data Protection Law, processing of personal data relating to criminal convictions,

offences and security measures may be carried out on the basis of the statutory provisions governing grounds for legitimate data processing only under the control of competent authority or, if a particular processing is allowed by law, if appropriate safeguards for the rights and freedoms of data subjects are undertaken. It is further envisaged that a comprehensive register of criminal convictions shall be kept only by and under the control of competent authority.

Anyhow, coming back to the regime of processing of special categories of data under the Current Data Protection Law, such processing is generally prohibited. However, this is not an absolute prohibition; this processing is allowed in certain exceptional cases explicitly prescribed by both the Current Data Protection Law and GDPR (Article 9) ("**Exceptional Cases**").

Specifically, the Exceptional Cases are the following:

1. The data subject has given explicit consent to the processing of such personal data for one or more specified purposes, except where a law provides that the processing cannot be performed on the basis of consent;
2. Processing is necessary for the purposes of carrying out the obligations or exercising statutory authorisations of the data controller or of the data subject in the field of employment, social security and social protection, if such processing is envisaged by a law or collective agreement which prescribes application of appropriate safeguards for the fundamental rights, freedoms and interests of the data subject;
3. Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
4. Processing is carried out as part of its registered activities with appropriate safeguards by a an endowment, a foundation, an association or any other not-for-profit organisation with a political, philosophical, religious or trade union aim, under the condition that the processing relates solely to the members or to former members of such organisation or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that organisation without the consent of the data subjects;
5. Processing relates to personal data which are manifestly made public by the data subject;
6. Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
7. Processing is necessary for reasons of substantial public interest, if such processing is proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
8. Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or the management of health or social care systems and services on the basis of a law or pursuant to contract with a health professional, if such processing is performed by or under surveillance of a health professional or of other person who has a professional secrecy obligation prescribed by law or professional rules;
9. Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border/boundary threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of a law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular with respect to professional secrecy;
10. Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 92, Paragraph 1 of the Law, if such processing is proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Accordingly, no processing of any personal data which belong to special categories of personal data is allowed if it does not "fit in" one of the Exceptional Cases.

Additionally, any processing of the respective data, when allowed, is subject to various additional obligations of data controllers/processors involved in their processing, such as, for example, potentially applicable obligation of conducting data protection impact assessment.

Specifically, it is explicitly prescribed that one of the cases when it is mandatory to conduct a data protection impact assessment prior to commencing a particular processing is the case when special categories of personal data are processed on a large scale. This is applicable irrespective of the fact which types of special categories of personal data are processed. On the other hand, a prior data protection impact assessment is also needed if the processing involves some particular types of special categories of personal data under some particular circumstances/for some particular purposes such as the processing of biometric data for the purpose of identification of employees by their employer, as well as when special categories of personal data (regardless of their type) are processed for the sake of profiling or automated decision making.

5. RIGHTS OF DATA SUBJECTS

The Current Data Protection Law envisages a set of rights which belong to data subjects in relation to their personal data processing. Exercise of these rights may be conditioned upon fulfilment of certain requirements and/or may be limited depending on the circumstances of each particular case. The law explicitly governs such requirements/limitations as well ("**Prescribed Restrictions**").

In general, subject to the Prescribed Restrictions, these are the following rights:

1. Right to request information on a particular processing;
2. Right to access to the processed data and to obtain their copy;
3. Right to rectification of the processed data;
4. Right to their erasure (*right to be forgotten*);
5. Right to restriction of the data processing (e.g. if the processed data accuracy is contested by the data subject);
6. Right to data portability (i.e. right to receive the processed data from the data controller in a structured, commonly used and machine-readable format, as well as to transmit them or to have them transmitted from one controller to the other);
7. Right to object to the data processing (e.g. if the processing is based on the legitimate interest or performed for direct marketing purposes) and to the processing cessation;
8. Right to withdraw consent (where consent is a legal ground for the processing), and
9. Right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning the data subject or significantly affects him/her ("**Relevant Rights**").

The majority of the Relevant Rights have already been recognised by the Old Data Protection Law, but some of them are completely new (e.g. right to data portability). In any case, data controllers are obliged to ensure exercise of the Relevant Rights (subject to the Prescribed Restrictions) and to do so within exact terms explicitly prescribed by the Current Data Protection Law (i.e. within 30-day period/up to 90-day period if extension of 60 days is necessary due to complexity and number of the requests for exercise of the respective rights). If they fail to fulfil their statutory obligation or comply with the relevant timeline, data subjects are entitled to file a complaint with the Commissioner ("**Data Processing Complaint**").

Also, any person who considers that any of his/her rights was infringed by processing activities of a data controller/processor, is entitled to the court protection of his/her rights.

It should also be noted that the Current Data Protection Law envisages a data subject right to damage remuneration. Specifically, any data subject who suffers a damage, material or immaterial, due to the processing of his/her personal data (regardless of their type or scope) performed by a data controller or data processor, is entitled to pecuniary remuneration of the suffered damage. This liability is primarily a liability of a data controller, but a data processor may be liable as well if it did not act in line with its statutory obligations or instructions issued by the data controller. Both of them can be released of liability if they prove that they are not in no way responsible for the occurrence of a particular damage.

The above-described concept of the respective rights is aligned with the GDPR (Chapter III – Rights of the data subject).

6. RECORDS OF PROCESSING ACTIVITIES

The obligation imposed by both the Current Data Protection Law and GDPR (Article 30) is the obligation of data controllers and data processors to keep records of their data processing activities.

These records should be established in a written form (including also electronic form) and should be kept permanently. They should also be made available to the Commissioner upon its request.

Their content is explicitly prescribed. Specifically, the following information on the processing should be generally included in these records:

1. Name and contact details of the data controller/processor and of its representative (if applicable) and of its DPO (if established);
2. Purpose(s) of the data processing; types of the processed data and categories of data subjects; categories of the data recipients;
3. Information (and related documents, if applicable) on the processed data transfer out of the economy;
4. Term of the processed data retention, if such term is established;
5. General description, where possible, of the security measures undertaken for the protection of the processed data, and certain other information explicitly prescribed by the law.

However, the obligation of keeping the respective records exists only if data controllers/processors have at least 250 employees or, regardless of their employee number, if the processing is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data or personal data relating to criminal convictions and offences.

Although the Current Data Protection Law imposes the above-described obligation of keeping records of processing activities, it does not oblige data controllers to register their databases containing personal data with the Commissioner. Such registration obligation was prescribed by the Old Data Protection Law (so-called Central Registry), and was applicable until the adoption of the Data Protection Law (i.e. until 21 November 2018) when the Central Registry ceased to exist.

7. DATA BREACH RELATED NOTIFICATIONS AND DATA PROTECTION IMPACT ASSESSMENT

Both the obligations regarding data breach related notifications and data protection impact assessment are novelties introduced by the Current Data Protection Law in line with the GDPR (Articles 33 – 36). None of them was envisaged by the Old Data Protection Law.

The fulfilment of these obligations depends on whether a particular processing (or a data breach) is likely to result in a risk or high risk to the rights and freedoms of natural persons.

If such risk would exist in a particular case, a data controller would be obliged to act as follows:

1. To notify (without undue delay or, if possible, within 72 hours) the Commissioner and/or data subject of a particular data breach (e.g. if an unauthorised person has accessed the processed personal data and made them available to general public), and
2. To carry out the assessment of an impact which a particular processing could have on the protection of personal data, prior to commencing such processing, whereas it is prescribed that the Commissioner shall establish and publish a list of the processing operations for which this assessment is required ("**Obligatory Assessment List**").

In this regard, it should be noted that the Obligatory Assessment List has been established – it is envisaged by one of the bylaws adopted upon adoption of the Current Data Protection Law (more information on this by-law and other secondary legislation adopted in relation to the Current Data Protection Law is provided under point 10 herein).

Also, when it comes to a data breach, a data processor is obliged to notify a data controller of a data breach without undue delay after becoming aware of the same.

8. DATA TRANSFER

A data transfer regime is one of the areas in which the biggest differences exist between the Current Data Protection Law and Old Data Protection Law.

Under the Old Data Protection Law, the crucial question was the question whether an economy to which the data is to be transferred is a member of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("**Convention**").

This Convention entered into force on 1 October 1985 (with five initial ratifications). It represents the first binding international instrument which intends both to protect individuals against abuses related to the personal data processing and to regulate the cross-border/boundary data flow. At the moment, the total number of the economies which ratified the Convention is 55. Serbia ratified the Convention on 6 September 2005 and it entered into force on 1 January 2006.

Under the Old Data Protection Law, if an economy to which the data is to be transferred from Serbia is a member of the Convention, a data transfer is free in a sense that no prior data transfer approval of the Commissioner is needed ("**Transfer Approval**"). If not, the only way for ensuring a lawful data transfer out of Serbia was to obtain the Transfer Approval prior to commencing it.

On the other hand, the Current Data Protection Law prescribes a set of mechanisms based on which a legitimate transfer of data out of Serbia is possible (with or without the Transfer

Approval). This means that the Current Data Protection Law tends, the same as the GDPR (Chapter V – Transfers of personal data to third economies or international organisations), to enable legitimate transfer of personal data whenever there are some safeguards that transferred data will be processed in line with the law.

Specifically, in brief, this means the following:

1. It should firstly be checked whether a particular economy to which the data is to be transferred is regarded as an economy with an adequate data protection system. Such economies are all the economies which are members of the Convention and all other economies which are on the list (so-called adequacy list) of the Serbian Government as the economies with adequate data protection regime (such as, for example, the EU and generally European economies, Israel, Japan, Canada (for business entities), etc.) ("**Adequate Economy**");
2. If an economy to which the data is to be transferred from Serbia is the Adequate Economy or if there is a data transfer related international treaty entered into between Serbia and that economy, a transfer is possible without the Transfer Approval;
3. On the other hand, if an economy to which the data is to be transferred is not the Adequate Economy, a transfer is still possible without the Transfer Approval if the adequate data protection measures are undertaken (e.g. if standard contractual clauses (SCC) prepared by the Commissioner have been entered into between a data controller as a data exporter and a data processor as a data importer or Binding Corporate Rules (BCR) approved by the Commissioner exist between the parties) ("**Adequate Safeguards**");
4. However, even if there are no Adequate Safeguards, there is still a possibility for transferring the data without the Transfer Approval. Such possibility exists in so-called special situations, explicitly prescribed by the Current Data Protection Law, the same as under the GDPR (Article 49). For example, if a data subject has consented to a particular transfer or if a transfer is necessary for the performance of an agreement between a data subject and data controller or if a transfer is necessary for the conclusion or performance of a contract concluded in the data subject's interest between the data controller and another natural or legal person or if the transfer is necessary for fulfilment of important public interest envisaged by the law, etc.);
5. Finally, even if none of the aforementioned special situations is applicable, a data transfer is still allowed without the Transfer Approval if certain conditions (linked to data controller's legitimate interest) explicitly prescribed by the Current Data Protection Law are cumulatively fulfilled. More precisely, these are the following conditions: (1) the transfer is not repetitive, (2) it concerns only a limited number of data subjects, (3) it is necessary for the purposes of the data controller's legitimate interest which prevails over the interests or rights and freedoms of the data subject, and (4) the data controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data.

The Transfer Approval still exists as a mechanism (obviously, considering all the above, only one of them) for ensuring legitimate data transfer out of the economy. This means that a data exporter may submit the contractual clauses for Commissioner's review with the aim to ensure adequate protection of transferred data and to transfer the data out of Serbia based on the Commissioner's approval of such clauses. The Commissioner is obliged to pass its decision on submitted request within 60 days from the day such request was submitted.

Under the Commissioner's Annual Report for 2019 (which is the last published report), available via the Commissioner's website www.poverenik.rs, 5 data transfer requests were submitted to the Commissioner in the course of 2019. 3 of these 5 requests were filed under the Old Data Protection Law, while the remaining 2 requests were filed under the Current Data Protection Law. These 2 requests relate to the data transfers from Serbia to Saudi Arabia and were processed/resolved in 2020.

Considering that 2020 is the first year during which the Current Data Protection Law is applied as of the year's beginning (which was not the case with 2019 since the Current Data Protection Law application began in the second half of 2019), it does not come as a surprise that only 2 data transfer approval requests (if the above Commissioner's report is fully accurate) were filed in the course of 2019.

It remains to be seen whether such number will increase in 2020 and if so, will it be a significant increase. However, we would not expect this to happen. The reasoning behind this position is the circumstance that, unlike the Old Data Protection Law, the Current Data Protection Law "offers" many other mechanisms for ensuring legitimate data transfer (e.g. adequacy decisions, standard contractual clauses, etc.) without any need to commence any procedure before the Commissioner.

In other words, we would say (and the practice shows the same, at least so far) that only if none of such other mechanisms would be available (due to the characteristics of a particular transfer), data controllers would opt for requesting a data transfer approval from the Commissioner (thus, probably only when having no other choice/option for ensuring legitimate data transfer out of Serbia).

9. PENAL POLICY

If we would have to identify the most significant difference between the Current Data Protection Law and the GDPR, the penal policy would certainly be the one.

This is due to the fact that, unlike very stringent penal policy and extremely high fines introduced by the GDPR (i.e. fines in the amount of up to EUR 20,000,000 or 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher), the Current Data Protection Law kept very mild penal policy.

Specifically, it prescribes offence liability for breaching the law, whereas the highest amounts of the fines for such breaches are RSD 2 million (approx. up to EUR 17,000) for a legal entity and RSD 150,000 (approx. up to EUR 1,300) for a legal entity's representative or a natural person, per offence.

Although offence liability under some other laws in force in Serbia includes, besides fines, certain additional sanctions/ protective measures (e.g. publication of a court decision, prohibition to perform certain business activities/duties within certain period of time), such additional sanctions/measures are not envisaged by the provisions of the Current Data Protection Law.

Additionally, it should be mentioned that the Law on General Administrative Procedure prescribes that if a legal entity to which a public authority (including the Commissioner in the field of data protection) ordered certain measures, does not fulfil such order, such legal entity may be fined in the amount of up to 10% of the respective entity's annual turnover generated in Serbia in the preceding year. However, for now, this legal remedy is of theoretical importance as we are not aware of its actual thus far application in practice.

Finally, criminal liability is also prescribed by the relevant Serbian legislation. Specifically, the Serbian Criminal Code introduces a criminal offence *Unauthorised collection of personal data*. The prescribed sanction is fine (in the amount to be determined by the court) or imprisonment up to 3 years. However, in general, criminal liability remains to be mostly a theoretical possibility (although some examples of filed criminal charges exist).

10. RELEVANT SECONDARY LEGISLATION

In addition to the Current Data Protection Law, a set of subordinate legislation (i.e. decisions and rulebooks) was adopted in the course of 2019 and 2020 ("**Adopted Legislation**").

The Adopted Legislation includes the following regulations adopted either in the course of 2019 or 2020 (the year of their adoption is stated in the brackets right after each of the respective regulation):

1. Decision on Determination of the Standard Contractual Clauses ("**SCC Decision**") (2020);
2. Decision on the List of Economies, Their Territories or One or More Sectors of Particular Business Activities in These Economies, and of International Organisations in Which It Is Considered that the Adequate Data Protection Level is Ensured ("**Decision on Adequate Economies**") (2019);
3. Rulebook on the Form and Manner of Keeping Records of Data Protection Officers ("**DPO Rulebook**") (2019);
4. Rulebook on the Form of Complaint (2019);
5. Rulebook on the Form of Data Breach Notification and on Informing the Commissioner of Information of Public Importance and Protection of Personal Data on Breach of Personal Data ("**Data Breach Rulebook**") (2019);
6. Decision on the List of Types of Data Processing Activities for which Data Protection Impact Assessment Must Be Performed and Opinion of the Commissioner for Information of Public Importance and Protection of Personal Data Must Be Requested ("**Decision on Data Protection Impact Assessment**") (2019);
7. Rulebook on the Form and Manner of Keeping Internal Record of Breaches of the Law on Protection of Personal Data and on the Measures Undertaken in the Performance of Inspection Supervision ("**Rulebook on Breaches of the Law**") (2019);
8. Rulebook on Identification of the Person Authorised to Perform Inspection Supervision under the Law on Protection of Personal Data ("**Rulebook on Inspection Supervision**") (2019).

This legislation governs the following issues introduced by the Current Data Protection Law:

I. **Data Processing Agreement** between a data controller and a data processor including also a transfer of processed data out of Serbia – the Commissioner prepared the model of the respective agreement, i.e. so-called **Standard Contractual Clauses (SCC)**. This model is envisaged by the SCC Decision, as defined above, which was adopted by the Commissioner and is applicable since January 2020.

   Under this Decision, the SCC have to be entered into in a written form (which includes electronic form as well). Considering that, under the Current Data Protection Law, any data controller seated in Serbia which intends to engage a data processor has to enter into a written data processing agreement with such processor, these SCC can be used as the respective agreement including also if the engaged data processor is a foreign entity – if a data transfer out of Serbia is involved.

   The SCC govern the following issues:

   1. Rights and obligations of both the data controller and data processor;
   2. Measures to be undertaken for ensuring protection of the processed data (e.g. pseudonymisation, encryption, ensuring permanent confidentiality, assessing efficacy of technical, organisational and human resources measures, etc.);
   3. Obligations regarding data breach notifications and data protection impact assessments;
   4. Rules for engagement of sub-processors;
   5. Rights of data subjects;
   6. Data transfer to other economies or international organisations;
   7. Monitoring of the data processor's work by the data controller;
   8. Duration of the processing;
   9. Obligations of the data processor upon termination of the agreed processing activities.

   The SCC should also contain a few Appendixes (structure and content of which is also prescribed by the aforementioned Decision) by which the following items should be governed:

   1. Particulars of the processing (such as types of the processed data, categories of the data subjects, purpose(s) of the processing, etc.);
   2. Description of the procedure which should be followed if the data processor considers that a written instruction obtained by the data controller is not compliant with the Current Data Protection Law and/or with the SCC provisions and of the consequences in the case of such illegitimate instruction;
   3. Description of the security measures;
   4. Obligations of the data processor with respect to the data breach notifications;
   5. Information on the engaged sub-contractors, if any;
   6. Information on the data transfer out of Serbia, if any;
   7. Information on the manner in which the data controller is to monitor the work of the data processor, and
   8. Information on the regime and terms for the agreement's cancellation.

   However, it should be noted that the SCC are applicable as a mechanism for ensuring legitimate data transfer out of Serbia solely if a transfer should be made from a Serbian data controller to a foreign data processor.

   In other words, if a data transfer out of Serbia is a controller to controller transfer, these SCC are not the applicable option. It is not clear why the respective provisions of the Current Data Protection Law were made to include such limitation; whether this was intentional or just an omission when the respective law was drafted. Anyhow, since there is no either legal or logical justification for such limitation, the respective provisions should be amended.

II. **Adequacy list for data transfer out of Serbia** - as mentioned under point 8 herein, the Serbian Government established the list of the economies which are regarded as the economies with adequate data protection system and to which the processed data transfer is free in a sense that no Transfer Approval is needed ("**Adequate Economies**").

   The respective list is prescribed by the Decision on Adequate Economies, as defined above, which was adopted by the Government and was applicable as of August 2019.

   Under this Decision, the aforementioned list includes two groups of Adequate Economies, as follows:

   1. Member states of the Convention (54 economies in total);

2. Economies/territories out of European Union for which it is established by the European Union that they ensure adequate level of protection (such as, for example, Israel, Japan, Canada (only with respect to business entities), New Zealand).

   Until recently, the USA (i.e. entities seated in the USA which are *Privacy Shield* certified entities) was also on this list, but this ceased to be the case upon the decision of the European Court of Justice by which the Privacy Shield was declared as ineffective/invalid for any further data transfers from any EU MS to the USA;

III. **Data Protection Officers** - in the cases when the DPOs, as defined under point 3 herein, are appointed, their contact details should be communicated to the Commissioner in the manner prescribed by the DPO Rulebook, which was adopted by the Commissioner and applies as of 21 August 2019.

Under this Rulebook, every data controller/processor which appoints its DPO should provide the Commissioner with the following information on the respective person: his/her full name, address, e-mail and phone number.

This information should be communicated to the Commissioner in writing, either by delivering it to the Commissioner or by sending it to by post or e-mail.

The Commissioner should keep the provided information within the electronic record the form of which is prescribed by the aforementioned Rulebook;

IV. **Communication with the Commissioner in specific cases** - the Data Processing Complaint, as defined under point 5 herein, and the data breach notification, as mentioned under point 7., should be filed with the Commissioner on the forms explicitly prescribed by the rulebooks. The respective rulebooks are the Rulebook on the Form of Complaint (2019) and the Data Breach Rulebook, as defined above. Both Rulebooks were adopted by the Commissioner and apply as of 21 August 2019.

When it comes to the Data Processing Complaint, it can be filed, on the prescribed form, by any natural person who considers that a particular processing of his/her personal data is performed contrary to the Current Data Protection Law.

The aforementioned form should be submitted to the Commissioner in writing, directly or by post or by e-mail prituzba@poverenik.rs, and it should contain the following information:

1. Information on the person filing a complaint;
2. Information on the data controller against which a complaint is filed;
3. Identification of the data subject's right(s) which was/were infringed by the respective illegitimate processing (e.g. right to access the data or to their rectification or deletion or data portability right, etc.), and
4. Identification of the reason(s) for filing a complaint (e.g. a data controller did not pass a decision on an objection previously submitted by the respective data subject).

When it comes to the data breach notification, it should be filed, whenever applicable, on the prescribed form as well, whereas such form should contain the following information:

1. Information on the data controller;
2. Information on the data breach (its description, types and number of the personal data to which it relates, number of the concerned data subjects and date and time when the breach occurred);
3. Description of possible consequences of the breach;
4. Description of the measures which the data controller has undertaken or they are proposed to be undertaken;
5. Other information relevant for a particular breach.

It is further described by the respective Rulebook that the data controller should notify the Commissioner of the breach, by submitting the above-described form, within 72 hours from the moment it becomes aware of it or, if it is not possible to submit the respective notification within such term, it should be explained why that was not possible.

Along with the data breach notification, the data controller should also provide the Commissioner with its records of data processing activities relating to the respective data, as well as with all other documents which may be requested by the Commissioner or which the data controller considers relevant.

In any case, the prescribed form should be filed with the Commissioner in writing, directly or by post or by e-mail.

V. **Data Protection Impact Assessment** – as mentioned under point 7 in this Section 2 of, the Obligatory Assessment List is explicitly prescribed.

The cases included in the respective list when it is obligatory to perform data protection impact assessment prior to commencing any processing, are the following:

1. Systematic and comprehensive assessment of the condition and characteristics of a natural person which is subject to automatic processing of personal data, including profiling as well, on the basis of which decisions are passed which are relevant for an individual's legal position or influence him/her significantly in a similar manner;
2. Processing of special categories of personal data or personal data relating to criminal convictions and offences and security measures, on a large scale;
3. Systematic monitoring of publicly available surfaces on a large scale;
4. Processing of personal data of children and minors for the purpose of profiling, automated decision making or for marketing purposes;
5. Use of new technologies or technological solutions for data processing or with possibility of data processing which serve for analysis or predictions of economic situation, health, affinities or interests, reliability or behaviour, location or movements of natural persons;
6. Processing of personal data in a way which includes monitoring of location or behaviour of individuals in the case of systematic processing of communication data made by the use of phone, Internet or other communication means;
7. Processing of biometric data for the purpose of identification of employees by employer and in other cases of processing of employee personal data by employer by using applications or systems for monitoring their work, movement, communication and similar;
8. Processing of personal data by their combining, connecting or checking compatibilities from different sources;
9. Processing of special categories of personal data for the purpose of profiling or automated decision making.

It is also prescribed that, in addition to the above-identified cases, a data controller shall be obliged to perform data protection impact assessment in other cases as well, as long as it is likely that a particular processing, considering nature, scope,

circumstances and purpose of the processing and particularly if new technologies are used, will cause a high risk to rights and freedoms of natural persons.

In any case, depending on the results of a prior data protection impact assessment, it may be necessary to obtain Commissioner's opinion in line with the Current Data Protection Law.

The relevant regulation is the Decision on Data Protection Impact Assessment, as defined above. This Decision was adopted by the Commissioner and applies as of 21 August 2019.

Besides the above-described secondary legislation, there are also 2 additional regulations which govern the following matters: (1) record of breaches of the Current Data Protection Law and measures undertaken as part of inspection supervision of the respective law implementation, and (2) identification of the inspectors authorised to act under the Current Data Protection Law and manner in which the record of the respective issued identifications is kept.

The Rulebook on Breaches of the Law governs the record of the Current Data Protection Law breaches, as defined above. It was adopted by the Commissioner and applies as of 21 August 2019.

The regulation governing the identification of the inspectors authorised to act under the Current Data Protection Law and the manner in which the record of the respective issued identifications is kept is the Rulebook on Inspection Supervision, as defined above. It was adopted by the Commissioner and applies as of 7 October 2019.

3. COMPETENCE OF AND CHALLENGES IN THE WORK OF THE COMMISSIONER

The public authority with the competence in the field of data protection is the Commissioner for Information of Public Importance and Protection of Personal Data (in Serbian, *Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti*).

For the sake of completeness and as already mentioned in Section 1 of this Chapter VI, the Commissioner is actually the authority with dual competence, whereas one of them is protection of personal data and the other is enabling/making sure care that access to information of public importance is enabled in line with the relevant law.

The Commissioner has two deputies and two counsellors, as well as an expert team which provides it the support needed for fulfilling its duties and competences ("**Commissioner's Office**"). An internal auditor is also part of the Commissioner's organisational structure.

The Commissioner's Office is consisted of seven departments:

1. Department for Harmonisation;
2. Department for Complaints and Enforcement – Access to Information;
3. Department for Protection of Rights of Persons and Data Transfer – Protection of Data;
4. Department for Information Technologies;
5. Department for Monitoring;
6. Department for Joint Activities;
7. Department for Cooperation and Reporting.

The total number of staff currently engaged with the Commissioner's Office is 91. Almost all of these persons, 89 of them, are employed with the Commissioner, out of which the majority (83) are employed for an indefinite period, while the remaining 6 employees are employed for definite period of time.

However according to Commissioner's internal systematisation rules the total of 129 of persons should be employed with the Commissioner; thus 30 people more than currently employed, which leads us to the conclusion that the current capacities of the Commissioner's Office are not sufficient. However, it should be kept in mind that the existing discrepancy between the current and planned number of employees is not the same for all the departments within the Commissioner's Office. For example, based on the information published on its website, one of the departments in which the discrepancy is most pronounced is the Department for Harmonisation as the current number of employees in this department is 10, while the planned number is 21, and the Department for Information Technologies which currently has only 2 employees, while the planned number is 11.

For the purpose of understanding the scope of work Commissioner's Office performs on a monthly basis, monthly statistical information should be consulted (they are published regularly on the Commissioner's website www.poverenik.rs).

For example, under the data published for September 2020, the relevant statistics is as follows:

1. The Commissioner's Office received 603 new matters in the course of this month out of which 131 was related to the protection of personal data;
2. Total number of the matters resolved in September 2020 was 516 in total, out of which 168 relate to the protection of personal data;
3. Total number of pending matters is 3,320 in total, our of which 183 relate to data protection matters;
4. Based on the records of the phone calls made in the course of the respective month, total number of phone contacts with both citizens and public authorities, in relation to both data protection and access to information of public importance, was 2,418.

The Commissioner is an autonomous public authority established in 2009. Under the Current Data Protection Law, it is declared to be completely independent in preforming its work and authorisations and free of any, direct or indirect, external influence and cannot request or receive orders from anyone. It also selects its employees and manages them independently.

Nevertheless, considering that the Commissioner is a public authority, financial resources for its work are provided from the government budget in line with the law on budget and laws governing public administration and position of public servants. Information on the exact purposes for which the budget resources provided to the Commissioner are spent (e.g. employee salaries, travel expenses, expenses for office equipment and materials, etc.) and on the exact amount of each of such spending is published on the Commissioner's website.

The Commissioner is also obliged to prepare an annual report on its activities and to submit such report to the National Assembly of Serbia, and such report is also delivered to the Serbian Government.

In this regard, it should be noted that the National Assembly is the authority which adopts laws, thus it adopted the Current Data Protection Law as well. Before commencement of such adoption process, a proposal of a particular law should be submitted to the National Assembly while one of the entities authorised to draft such proposal is the Serbian Government. In the case of the Current Data Protection Law, the respective proposal law was drafted by the Ministry of Justice as one of the ministries within the Government.

In any case, upon being adopted, the law enters into force on the eight day upon being published in the Official Gazette of the Republic of Serbia at the earliest (subject to certain

exceptions). On the day the law enters into force, it begins to apply as well; however, this is not always the case. Specifically, it may happen that, due to complexity of a particular law, substantial changes which it introduces or some other relevant circumstances, a law enters into force on one day and becomes applicable on the other, later date. Precisely this is the case with the Current Data Protection Law. The period between the date the law was adopted (21 November 2018) and the date the rules envisaged by it (subject to certain exceptions) became applicable (21 August 2019) was nine months. This was the so-called transitional period left for the data controllers/processors to align their operations in relation to the personal data processing with the rules envisaged by the Current Data Protection Law. For the purpose of comparison, the transitional period under the GDPR was much longer, i.e. data controllers/processors had the period of 24 months to become compliant with the GDPR.

The Commissioner's competences are set in detail by the Current Data Protection Law. They are numerous and include, amongst other, monitoring the respective law implementation, raising public awareness with respect to the rules, risks, measures of protection and rights in relation to the processing of personal data, acting upon complaints of data subjects, preparing the so-called standard contractual clauses (SCC), approving the so-called binding corporate rules (BCR), keeping internal records of appointed DPOs and of the Current Data Protection Law breaches and measures undertaken as part of the inspection supervision, etc..

For the purpose of exercising its authorisations and duties within its sphere of competence, the Commissioner has two types of powers:

1. Powers relating to its capacity of a second-instance authority responsible for protecting the right to data protection in appeal proceedings (i.e. based on the Data Processing Complaints filed with the Commissioner) ("**Appeal Related Powers**"), and
2. Powers relating to its capacity of a supervisory authority responsible for enforcing the Current Data Protection Law ("**Supervisory Powers**").

When it comes to the Commissioner's Appeal Related Powers, it decides on filed complaints within 30 days from the day of their filing, whereas it firstly forwards the complaints to the data controller(s) responsible for undertaking data processing activities which the complaints were filed against for their comments. Depending on the fact whether the Commissioner finds a complaint grounded, it may reject the complaint (if ungrounded) or order the data controller to act upon request within a specified period of time (if grounded). In any case, no appeal can be filed against a decision passed by the Commissioner, but an administrative dispute can be initiated against such decision (or if the Commissioner does not pass a decision within the statutory term) before the competent court.

When it comes to the Commissioner's Supervisory Powers, the Commissioner is entitled, amongst other, to order certain corrective measures to data controllers/processors (e.g. to order them to stop undertaking particular data processing activities), as well as to file a request for initiating offence proceedings against them before the competent court.

Additionally, the Current Data Protection Law also establishes (which is a significant difference in comparison to the Old Data Protection Law) the Commissioner's competence to issue fines for certain offences directly (e.g. if a foreign data controller/processor to which the Current Data Protection Law is applicable does not appoint its representative for the territory of Serbia). The sanction prescribed for such offences is a fine in the fixed amount of RSD 100,000 (approx. EUR 850) per offence.

It should further be noted that cooperation of the Commissioner with other authorities is of substantial importance for adequate implementation of the Current Data Protection Law and further development of data protection law in Serbia.

This is due to the fact that processing of personal data is an integral part of a day-to-day operations of numerous business entities and institutions, as well as of both public and private sector, such as, for example, in the field of telecommunications, healthcare, education, banking, insurance and many other. This further means that applicable sectoral laws should be fully harmonised with the terms and requirements of the Current Data Protection Law.

In this regard, it should be mentioned that it is explicitly prescribed by the Current Data Protection Law that provisions of all other laws which govern processing of personal data have to be aligned with the Current Data Protection Law by the end of 2020.

Further, the support (other than the aforementioned government budget allocation) the Commissioner (potentially) receives for the purpose of further development of data protection policies and practice in Serbia is important for its work and organisation.

Based on the information publicly available on Commissioner's website www.poverenik.rs, the Commissioner participated in a few important and successfully implemented projects in the period from 2010 to 2018. These are:

1. **Strengthening Accountability Mechanisms in Public Finance** project which the Commissioner implemented in cooperation with the United Nations Development Programme (UNDP) in the period from April 2010 to June 2012;
2. **Protection of Whistleblowers** project which the Commissioner implemented in the period from July 2012 to November 2013 with the funding from the British Embassy in Belgrade and the Government of the Netherlands;
3. **Improvement of Personal Data Protection** project which the Commissioner and Information Commissioner of the Republic of Slovenia implemented in the course of 2012 and which was funded by the European Union Instrument for Pre-Accession Assistance (Twinning Project IPA 2009 Project No. SR/2009/IB/JH/01TWL);
4. **Building of Capacities of the Commissioner for Information of Public Importance and Protection of Personal Data for Effective and Adequate Fulfilment of Its Statutory Authorisations and for Ensuring Exercise of the Rights of Free Access to Information and Protection of Data in Compliance with the European Standards**, which was implemented based on the Project Implementation Agreement no. 37-00-00018/2015-04/1 entered into between the Commissioner and European Integration Office of Serbia on 18 September 2015, funded from the resources provided by the Kingdom of Norway (based on the bilateral agreement entered into between Norway and Serbia), as part of which many training sessions for the Commissioner's staff were held in the course of 2016, 2017 and 2018 (such as the training in the field of data protection, privacy, free access to information, human resources, copyrights, EU regulatory framework and practice, video surveillance, digital forensics, and other).

No project is published on the Commissioner's website as currently being underway. Consequently, it seems that there are no such projects at the moment.

In addition, when it comes to existing cooperation between the data protection authorities in the region, Initiative 2017 should be mentioned. This group is consisted of data protection authorities from the following seven jurisdictions in the region: Serbia, Montenegro, Bosnia and Herzegovina, Republic of North Macedonia, Croatia, Slovenia and Kosovo*. So far, 3 meetings of the group were held. The last one was held from 26 May to 28 May 2019 in Montenegro and focused on then current state of alignment of the respective jurisdictions' legislation with the GDPR. It remains to be seen how much/whether this group (and the Commissioner as its part) shall be active in the future, considering particularly the fact that some of the aforementioned jurisdictions have not adopted their GDPR aligned laws yet such as Bosnia and Herzegovina and Montenegro.

Finally, with regard to the Covid-19 pandemics which is on-going not only in Serbia, but all around the region and whole world too, it should be noted that the Commissioner undertook certain activities/made related announcements (and still does) via its website www.poverenik.rs regarding processing and protection of personal data under such specific and challenging circumstances (there is a special section on the website dedicated to Covid-19 titled Covid-19 and Protection of Personal Data).

Specifically, at the very beginning of the pandemics (at the beginning of March 2020), the Commissioner called the media not to publish personal data of individuals infected by the virus because, as stated in the respective Commissioner's announcement, information on the infected citizens of Serbia have been published in a way that the identity of those persons could be determined or is determinable. The Commissioner emphasised that, besides the fact that publishing of such information is contrary to the Law on Public Information and Media, the respective data are health related and, as such, fall within special categories of personal data the processing of which is subject to significant restrictions

Considering that the state of emergency was declared in Serbia in March 2020 (it lasted for a few months), at the beginning of April 2020 the Commissioner issued the announcement emphasising, amongst other, that even in the course of the state of emergency all data controllers and data processors are still obliged to process personal data in compliance with the Current Data Protection Law and other relevant regulations and that data subjects are entitled to request exercise of their statutory rights related to data processing.

The Commissioner stayed active even after the cancellation of the state of emergency – the aforementioned section of its website dedicated to Covid-19 contains much information on the data processing during the pandemics, and various articles and related studies, both at local and international level.

For the sake of completeness, it is also worth mentioning that, besides the field of data protection, the Commissioner's active engagement related to the specific Covid-19 circumstances is noticeable in the second field of its competence – access to information of public importance.

Amongst other, it was announced on the Commissioner website that the number of citizen's complaints (relating to access to Covid-19 related information of public importance) has significantly increased after the cancellation of the state of emergency.

Further, it was recently published that the Commissioner participated in the first regional conference "Initiative 2020" held on 20 October 2020 at the initiative of the data protection authority of Slovenia. The purpose of this initiative is cooperation and exchange of good practice as regards promotion and protection of the right to access information of public importance. Initiative 2020 is similar to the Initiative 2017 previously established at the regional level in the field of data protection.

Considering the above initiatives, and projects completed and generally regular cooperation between the data protection authorities in the region, as well as the fact that the respective jurisdictions have already, the same as Serbia, adopted the GDPR aligned laws (such as, for example, the Republic of North Macedonia) or should (relatively) soon do so (such as, for example, Montenegro), we do not perceive any particular cross border/boundary data protection issues (of pure legal nature, (possible) political restraints aside) which should be regarded as unsolvable or burdensome in the region.

For the avoidance of any doubt, the precondition which should be fulfilled for the realization of the above cross-border/boundary data protection "scenario" in the region is that the local data protection laws (already aligned with the GDPR or about to become aligned) should be duly, consistently and continuously applied and implemented, the same as any other regulations adopted on the basis of the respective laws, by the data protection and other relevant authorities in each of the jurisdictions. Amongst other, this means that local authorities would not develop/support any practice/requirements which would be harsher for data controllers/processors in comparison to the requirements introduced by the GDPR (and, thus, by the local data protection legislation as well). Otherwise, the environment of legal uncertainty may be created and such environment would certainly not be the ground for further development on either local or, particularly, regional level.

4. CHALLENGES IN THE IMPLEMENTATION OF THE CURRENT DATA PROTECTION LAW IN PRIVATE AND PUBLIC SECTOR

The challenges in the implementation of the Current Data Protection Law ahead of the Local Processing Entities in both private and public sector are numerous.

In general, the most difficult ones are those linked to the full and adequate implementation of the principles of accountability and data protection by design and default, as envisaged by the Current Data Protection Law. The reasoning behind this position is further elaborated in this Section 4.

At the same time, the penal policy introduced by the Current Data Protection Law is very mild. It can freely be said that it is symbolic in comparison to the draconian fines imposed by the GDPR. Moreover, there is also a low level of enforcement, so it can easily happen that the level of compliance with the data protection requirements imposed by the Current Data Protection Law would be as low as it was with respect to the Old Data Protection Law.

Also, the level of public awareness about the importance of personal data protection and knowledge of the rights of individuals as data subjects is rather low as well.

Considering such circumstances, data controllers and data processors in Serbia (on which significant obligations are imposed by the Current Data Protection Law) may ask themselves why to invest resources and efforts in reaching full compliance with the respective law, if there would be, due to very mild penal policy and low level of enforcement, no or at least no significant consequences for their non-compliance.

Before providing information on the crucial steps to be undertaken for the purpose of avoiding such scenario – avoiding that the environment of non-compliance would become/remain the "normal" state of affairs which does not lead (and/or is not perceived to lead) to any actual fines, other sanctions or any other relevant consequences regardless of the breaches of the law which may have been committed, the existing challenges in the implementation of the Current Data Protection Law, as generally identified above, should be further elaborated.

Specifically, some of the respective challenges are new (as they occurred due to the novelties introduced by the Current Data Protection Law) ("**New Challenges**") and other are old (as they existed already at the time the Current Data Protection Law was adopted) ("**Old Challenges**").

With regard to the New Challenges, it should be noted that the novelties introduced by the Current Data Protection Law led to various obligations of both data controllers and data processors. Some of the most important novelties are the following:

1. Broadening the scope of the data subject's rights – introducing some completely new rights (such as data portability right) and putting emphasis on, amongst other, transparency towards data subjects;
2. Data breach notifications towards the Commissioner and/or affected data subjects, depending on the characteristics of a particular breach, and introduction of tight deadlines (72 hours) for fulfilling the respective obligations;

3. Performance of data protection impact assessments and requirement to obtain, depending on the outcome of the respective assessments, related opinion of the Commissioner prior to commencing the respective processing;
4. Appointment (obligatory or voluntary) of data protection officers as the Local Processing Entities' contact points towards both the Commissioner and data subjects, and, when it comes to foreign entities to which the Current Data Protection Law is applicable, obligatory appointment (subject to certain exceptions) of data protection representatives;
5. Enhanced security related obligations including data protection by design and default;
6. Responsibility of data controllers for demonstrating their compliance with the requirements imposed by the respective law (accountability principle).

The most demanding of the above obligations/responsibilities is to implement the principles of accountability and data protection by design and default, as already mentioned at the beginning.

This is due to the fact that the implementation of respective principle would require the Local Processing Entities to respect the data protection requirements from the creation/further development of their IT system as, otherwise, they would not be able to respond to or address the challenges which the Current Data Protection Law imposes (such as, for example, the requirement to ensure exercise of the data subject's rights and to ensure such exercise is made within the terms envisaged by the law, or requirement to timely prepare and file data breach notifications).

Accordingly, full and adequate implementation of the Current Data Protection Law requires significant resources (e.g. for obtaining adequate equipment/software and hiring qualified personnel) for the vast majority of the Local Processing Entities.

The data minimisation principle should also be mentioned. Its implementation may be challenging in practice, both in private sector and in public sector, considering that various types of records/registries are kept by the Local Processing Entities containing much personal data, whereas not all of them are absolutely necessary for the fulfilment of their legitimate processing purposes. Minimising the retention terms whenever possible (as sometimes long retention periods or even permanent keeping are prescribed as mandatory) will be a challenge of its own.

With regard to the Old Challenges – those "inherited" from the time prior to adoption, entry into force and application of the Current Data Protection Law, the most important ones are:

1. Low public awareness on data protection importance and of available legal resources;
2. Low level of enforcement;
3. Mild penal policy.

When it comes to the challenge of low public awareness on data protection importance and of available legal resources, as well as the challenge of low level of enforcement, it does not mean that that there is absolutely no awareness/activities in this regard, on the contrary, but their further development/intensification is certainly needed.

By way of illustration, and given the situation in the last two years, it should be noted that the total number of complaints filed with the Commissioner due to breaches of the data protection right (under both the Old Data Protection Law and Current Data Protection Law) is:

Year	Number of Filed Complaints
2019	181
2020	85

This information is published on the website of the Commissioner www.poverenik.rs within the *Communique on the Commissioner's Work* of 31 August 2020 ("**Commissioner's Communique**").

The *Commissioner's Communique* also contains the information relevant for measuring the level of enforcement in the course of the last two years – number of misdemeanour procedures initiated due to committed breaches of the law (Old Data Protection Law or Current Data Protection Law) is:

Year	Number of Initiated Misdemeanour Procedures
2019	23
2020	4

It is interesting to mention that, based on the information available in the Commissioner's Communique, even a few criminal charges were filed, 3 in 2019 and 2 in 2020. However, no further details on the course/outcome of the respective proceedings are published.

Further, the number of inspection supervision procedures ("**Inspections**") initiated (and measures issued by the Commissioner) with respect to the implementation of the Current Data Protection Law in the course of the last two years, are as follows:

Type of the Inspection	Number in 2019	Number in 2020
Inspections initiated upon request	43	92
Inspections initiated upon other ground	5	15
Inspections initiated upon warning of the competent authority	2	1
Inspections initiated upon request of the inspected entity	2	12
Inspections in the premises of data controllers	32	59
Type of the Measure	**Number in 2019**	**Number in 2020**
Measure of Limiting Processing Activities including Processing Prohibition	/	5
Measure of Warning Issued to Data Controller due to Breach of the Law	6	42
Inspection Order	31	80
Notification of Forthcoming Inspection	30	69
Request for Written Statement	1	97

Based on the above number of inspections which were initiated and of measures which were undertaken by the Commissioner in the course of 2020 (in comparison to 2019), a positive development can be noticed.

It remains to be seen how the situation will develop until the end of 2020 and later on, as well as whether the penal policy will remain mild as it, in general, used to be so far. In this regard, it should also be noted that mild penal policy is, generally speaking, not only characteristic of data protection legislation, but of fields of law as well.

5. CRUCIAL STEPS FOR OVERCOMING THE EXISTING CHALLENGES

The crucial steps to be undertaken for overcoming the above-described main challenges in the implementation of the Current Data Protection Law are the following:

1. Raising public awareness on the data protection importance (in particular when it comes to the rights data subjects have under the Current Data Protection Law, but in general as well), whereas this should further lead to the more significant reputational risk for the Local Processing Entities;
2. Harmonisation of all laws and other regulations which govern any processing of personal data with the terms and requirements imposed by the Current Data Protection Law;
3. Regular and continuous education and training of individuals involved in the processing of personal data both in the public and private sector;
4. Intensification of the inspection supervision of the Current Data Protection Law implementation (to the extent possible considering the existing staff restraints faced by the Commissioner);
5. Commencing and conducting offence proceedings before the competent courts against all data controllers/processors breaching the law;
6. Emphasising possible applicability of the GDPR, due to its extraterritorial effect, to the Local Processing Entities as well.

Further details regarding the above crucial steps for overcoming the most important challenges for further development of local data protection law and practice, and measures covered, are provided below.

- **Education of the public** is the starting point and one of crucial mechanisms for further development of data protection law and environment.

  It can be carried out, amongst other, by media campaigns, as well as by data protection training which could start even in schools, for which purpose the Commissioner could cooperate with the Ministry of Education, Science and Technological Development.

- Furthermore, the Commissioner should be very proactive and continue issuing reports and publishing such reports, but also relevant notifications and news (relating to Serbia, but covering the European Union/international perspective as well) on its website, as well as educational videos, podcasts, articles, handbooks, check lists.

  Publication of the most relevant information and developments should be continuously made through social networking platforms, since such platforms are widely used by the general public and communications made through them is expected to reach many concerned individuals.

  Additionally, the tool which would significantly help in the process of raising awareness about data protection is a platform for questions and answers. This platform should be available to everyone to submit a question to the Commissioner, which would then be responded and saved on the platform where any interested person could access and search through the data protection questions most frequently asked (FAQ). The FAQ section already exists on the Commissioner's website.

  Overall transparency and proactive approach of the Commissioner are of crucial importance not only for raising the level of public awareness and further education of the public, but also for strengthening trust of the public in the Commissioner itself.

- It may also be useful to conduct a **study on the level of data protection awareness** of the general public. This would offer a clear overview of the current situation, according to which the necessary steps for increasing awareness can be tailored.

- All the above is very important because data subjects would be able, only if properly educated, to (1) understand the importance of adequate data protection and seriousness of the risks (e.g. identity stealing risk) to which they may be exposed if their data would be processed contrary to the relevant legal requirements, and to (2) react adequately and timely should any breach of the Current Data Protection Law occur (e.g. by filing a complaint with the Commissioner or damage remuneration lawsuit with the competent court).

  They should also be aware of their rights in respect to the Local Processing Entities which may process their data, because, without adequate knowledge of such rights, they would not be able/not know how and when to use them.

  Their knowledge and reactions in the cases when they consider that some illegitimate activities are undertaken would further influence the Local Processing Entities to be more careful and to act in compliance with the Current Data Protection Law. Otherwise, they could be exposed to the inspections by the Commissioner (and, consequently, other government authorities/competent inspectors), court procedures, offence and other legal liability, as well as to significant reputational risk (which is often more important than material damage/fines which they may be obliged to remunerate/pay).

- For this reason, **the Local Processing Entities** would also need **to take care of regular and continuous education and training of their own employees**.

  This is equally applicable regardless of the fact whether the Local Processing Entities are part of private or public sector, thus equally applicable to government authorities/institutions as well, particularly if they are involved in the processing of special categories of personal data such as, amongst other, health related data.

- **Continuous education of the staff in the Commissioner's Office** is very important as well, as such education is a prerequisite to ensure they can keep pace with the newest developments in the field of data protection law and improve local data protection environment to the maximum possible extent.

  For this reason, the Commissioner should take active participation in international events and forums, as well as participate in and take initiatives for joint activities with data protection authorities from other economies.

  The important role of the Commissioner can be strengthened, especially in the eyes of entities and natural persons, if the public sector sets an example of trust, compliance with the measures, observations, recommendations, opinions and instructions of the Commissioner.

  Further increase of the number of the employees in the Commissioner's Office should be considered as well.

- It should be constantly emphasised that the **GDPR** itself may be fully applicable to the Local Processing Entities due to its **extraterritorial effect**.

  Considering constant intensification and development of online sales activities (due to the Covid-19 pandemics as well), the possibility of the GDPR's application to the Local Processing Entities becomes stronger than ever, in particular if their e-sale channels/on-line shop services are to be offered and available not only to local customers, but to those in the European Union as well. Further development of an active cooperation with other data protection authorities, especially in the European Union, is advisable.

  Further, although the Current Data Protection Law is the GDPR aligned law, it is necessary that the process of alignment covers all other laws and regulations governing data processing activities. In other words, such **legislation should be harmonised with the terms and requirements imposed by the Current Data Protection Law**.

  In this regard, it should be noted that it is explicitly prescribed by the Current Data Protection Law that provisions of all other laws which govern processing of personal data have to be aligned with the Current Data Protection Law by the end of 2020.

As the end of 2020 approaches, it will be soon seen whether such alignment has indeed been achieved. In any case, it is important to emphasise that the respective alignment should not be viewed solely from the perspective of introduction/amendment of the relevant provisions in the relevant laws, but it should also be checked whether the relevant rules/restrictions are indeed applied and fully respected in practice.

For example, it is certainly relevant, but definitely not sufficient, that local data controllers adopt internal acts compliant with the requirements of the Current Data Protection Law and other relevant regulations. However, the respective adoption will be of substantial relevance only if data controllers also establish mechanisms/implement safeguards and other measures which will enable efficient implementation of data protection principles and of the rights and obligations of both data controllers (and data processors, if engaged) and data subjects in line with the law.

- Additionally, **regular communication and cooperation between relevant authorities** is of principal importance in practice, not solely when such cooperation is formally prescribed as obligatory (e.g. in the form of regular reports obligatory for submission to the Commissioner), but also in the broader sense of sharing knowledge and discussing current issues and mechanisms for addressing them jointly to the extent feasible.

  Lack of such communication and cooperation would certainly represent a burden (if not even a showstopper, at least to a certain extent) for overall development of data protection law in the economy and for full implementation of the processing principles and rules envisaged by the Current Data Protection Law (and, thus, of the principles and rules introduced by the GDPR).

- When it comes to the **public sector**, we would also like to point out to one important process in which personal data processing perspective should be duly taken care of. Such process is **digitalisation** and introduction/further development of e-governance projects/platforms.

  Digitalisation is announced as one of the priorities of the Serbian Government. This is fine and in line with global trends, but it must not be forgotten that, besides the technological perspective which is of utmost importance, the data protection perspective should be taken care of equally.

  This means that the software/e-platforms must be designed in a way that the principal GDPR requirements (and, thus, requirements of the Current Data Protection Law as well) are duly respected. The principles of data minimisation and transparency, as well as of security should be addressed particularly.

  The use of new technologies for the respective purposes would most probably need to be subject to the prior data protection impact assessment and opinion of the Commissioner. This should be coordinated with the Commissioner and it should be generally consulted in order to ensure that all relevant aspects of data protection law are duly considered.

- With regard to the present **penal policy**, as envisaged by the Current Data Protection Law and other relevant regulations, we believe that it should include, besides the existing fines (which, obviously should be much higher than they currently are, but, then again, they need to be within boundaries set by the legislation governing offences in general), some additional sanctions, such as protective measures with regard to offence liability. Specifically, various protective measures are envisaged by different Serbian laws in various fields/sectors as sanctions which may apply in addition to fines.

  These measures include, amongst other, publication of court decisions passed against entities breaching a law and prohibition to perform business activities for certain period of time.

  The former (publication of court decisions) should serve to boost reputational risk for entities breaching the law as such risk is often more important that the fine/any particular sanction which may be adjudicated in the case of established liability for breaching the Current Data Protection Law.

  The latter (prohibition to perform business activities for certain period of time) should be used for particularly harsh cases when data protection breaches may lead, due to the types of the processed data or their scope or any other relevant characteristics of a particular processing, to significant consequences in private and professional life of data subjects.

- Additionally, the measure which may also be relevant and effective, at least when it comes to those of the Local Processing Entities which are private entities that participate regularly, due to the types of their business activities, in **public procurement procedures**, is the measure of establishing data protection related offences/previously established liability of a bidder for **data protection breaches** as the circumstance which may influence its ability to participate in public procurements and be awarded the respective agreements by the procurement entity.

The above-identified measures are only some of the numerous measures which may be further discussed and considered for further enhancement of current data protection regulatory framework and environment.

Overall, the pillars of the respective development process remain to be EDUCATION (as the starting point for improvements in any field, thus, in the field of data protection law as well), whereas this should be a multi-level approach including data subjects, processing entities and competent authorities, and ENFORCEMENT (as the support by the entire system is absolutely necessary for achieving the best results and applying the most relevant and fully adequate sanctions).

If individuals as data subjects (regardless whether they are consumers, employees or simply citizens in their everyday life) would be aware of the importance which adequate protection of personal data has for their lives and if they would be aware of the risks (e.g. identity stealing risk) which unauthorised processing/misuse of personal data may expose them to, and if they would have sufficient knowledge of the statutory rights which belong to them as data subjects, they would certainly boost the existing data protection environment.

By reacting to potential non-compliant activities of local data controllers/processors adequately, regularly and timely, they would exert pressure on the respective entities to be more careful and more compliant with the Current Data Protection Law when it comes to their processing activities (in particular from the perspective of the types and scope of the processed data). Otherwise, as already mentioned above, they could be exposed to the inspections by the Commissioner (and, consequently, other authorities/competent inspectors), legal liability and significant reputational risk.

Of course, no goal could be achieved without proper ENFORCEMENT. Regardless of their level of knowledge and awareness data subjects need to be supported by the entire system - by competent authorities as only these can ensure that breaches of any law (thus, of the Current Data Protection Law as well) are sanctioned fully and adequately.

PART III. KEY FINDINGS AND CONCLUSIONS

Based on the comprehensive analysis of the data protection legislation in force in the Western Balkans economies ("**WB Economies**") and of the broader data protection environment and practice in each of them, it can be concluded that significant similarities exist between the WB economies in the field of data protection law. Having said this, the following key findings are identified:

1) DIFFERENT LEVELS OF ALIGNMENT OF THE LOCAL LEGAL FRAMEWORK WITH THE GDPR

The WB economies are divided in two groups depending on the circumstance whether they are at the very beginning of their GDPR alignment path or have already made some steps towards the alignment. The crucial criterion here is whether a GDPR aligned law has already been adopted in a particular WB economy or not.

Following the above criterion, the first group includes respective economies in which a GDPR aligned law has already been adopted. These are: Serbia, Kosovo* and Republic of North Macedonia. Considering that they already have their GDPR aligned laws, they should, subject to specifics of each of the respective economies, undertake the steps towards further alignment of their other relevant legislation with the data protection principles and rules envisaged by their GDPR aligned laws and/or towards adoption of the related secondary legislation and/or completion of the establishment of their data protection authorities as fully operational bodies (which is the case for Kosovo*) or further strengthening of capacities of their already existing and fully operational data protection authorities (Serbia and Republic of North Macedonia).

On the other hand, the second group includes respective economies in which a GDPR aligned law is yet to be adopted, whereas such adoption is generally expected to happen in the course of 2021. These are: Albania, Bosnia and Herzegovina and Montenegro. Obviously, the first challenge ahead of these economies is the adoption of a GDPR aligned law. The next steps are similar if not the same as those for first group: further alignment of their other legislation with the GDPR principles and rules, adoption of the relevant secondary legislation and further strengthening of capacities of their data protection authorities to be able to address the challenges which shall be imposed on them upon the adoption of their GDPR aligned data protection laws.

2) LOW LEVEL OF PUBLIC AWARENESS ON THE IMPORTANCE OF DATA PROTECTION AND ON AVAILABLE LEGAL RESOURCES

One of the most noticeable characteristics of a data protection environment in each of the WB economies is a generally low level of public awareness about the importance of adequate data protection, but also of knowledge/usage of available legal resources in case personal data is processed (or perceived to be processed) in contravention to the data protection law.

This is, subject to specifics of each particular WB economy, due to a combination of factors, but the following ones seem to be of crucial importance: (1) protection of personal data and compliance with the data protection and privacy requirements is still regarded by local data processing entities, including both in private sector and public sector, as an obligation of formal/administrative nature rather than as a substantial one (in particular when it comes, where applicable, to the registration of local data controllers/locally established databases containing personal data, with the local data protection authorities), (2) non-compliance with the data protection rules and requirements does not lead to any significant legal or any other consequences, (3) local data protection authorities are not as active and transparent in their work as they should be.

In any case, regular and continuous education and training of individuals involved in the processing of personal data both in the public and private sector, but also of general public/data subjects, is a key activity for changing the current condition.

3) LOW LEVEL OF ENFORCEMENT

One of the key reasons for generally low level of compliance with local data protection and privacy requirements is a low level of enforcement. As already elaborated n the Economy Reports provided for each of the WB economies individually, this does not mean, subject to specifics of each particular economy, that there is no enforcement at all, but that the level of such enforcement should certainly be higher that it currently is.

Accordingly, inspection supervision of the local data protection law implementation should certainly be intensified and should be undertaken, including the application of the prescribed sanctions, towards local data processing entities in both private and public sector equally.

4) MILD PENAL POLICY

When speaking about the key reasons for generally low level of compliance with local data protection rules and regulations, low level of enforcement is certainly not the only one; on the contrary, it should always be regarded jointly with a generally mild penal policy. Both in terms of the type/amount of the prescribed sanctions, and of their applicability in practice, this means that not only that the types of the prescribed sanctions are generally not as stringent as those envisaged by the GDPR, but also that, even when imposed, they are, when it comes to fines, lower than they could/should be.

This is applicable, subject to specifics of each particular WB economy, to both WB economies in which the GDPR aligned data protection laws have already been adopted and to those in which this is not the case yet. We would say that this is due to a combination of various factors including those which are not of legal nature, such as economic and social, but there is no doubt that achieving the higher level of implementation of local data protection laws, is closely and inevitably linked to the mild penal policy and low level of enforcement in the respective economies.

5) CAPACITY BUILDING NEEDS

All the above brings us to the challenge which is immanent to the current status of the local data protection authorities in all WB economies – challenge of insufficient resources of the respective authorities for efficient implementation of the local data protection laws. This is particularly the case as regards the staff of the respective authorities in terms of their number, particularly, although not exclusively, in the field of inspection supervision of law implementation. Insufficiency of other resources, such as adequate official premises and official vehicles, is also mentioned in the Economy Reports as the needs of the competent authorities in some of the WB economies. The need of further/regular and continuous education and training of the local data protection authority staff is identified as the need to be taken into consideration.

Accordingly, capacity building needs are evident and regardless whether such needs exist to the greater or lesser extent, they need to be addressed. Solely if they are adequately addressed, along with all the above-identified challenges, the relevant impact to and significant improvement of the current data protection practice and environment can be achieved.

Considering the above-identified key findings – similarities between the WB economies, the crucial steps for overcoming the existing challenges (these steps are described in detail in Part II of this report for each of the WB economies individually) are, consequently, similar if not the same in each of all WB economies.

In addition to all such steps, the importance of regional perspective of data protection development should be particularly emphasised given that one of the leading GDPR objectives is to enable free movement of personal data across jurisdictions. The only way to accomplish that goal in the Western Balkans region is regular and continuous cooperation between the data protection authorities of respective economies and the relevant European Union authorities and institutions, but also among the data protection authorities of WB economies. In this respect, it is of utmost importance that none of the WB economies prescribes any measures/rules stricter that those envisaged by the GDPR, towards any of the other WB economies and introduces no obstacles towards cross-border/boundary data processing operations involving any of other WB economies, for simply political or any other reasons beyond legal ones. This perspective and overall transparency should be an integral part of further development of data protection law and environment in all of the WB economies.

Accordingly, the following actions should be undertaken at the regional revel as priority:

I. Organising regular meetings of the representatives of local data protection authorities for the purpose of addressing joint needs, as well as for identifying the most important issues and finding the optimal solutions;

II. Sharing knowledge and experience in the field of data protection law continuously and transparently;

III. Monitoring developments in the field of data protection law and practice, particularly on the level of the European Union, including, without limitation, issued guidelines of the European Data Protection Board and positions and practice of the EU MS supervisory authorities, but also the requirements imposed by the EU Data Protection Enforcement Directive[30] as regards data processing performed by the authorities in the field of prevention, investigation, detection or prosecution of criminal offences/execution of criminal penalties, as well as national data protection legislation of the EU member states;

IV. Considering recommendations and assessments introduced by the European Commission's European Data Strategy and, accordingly, keeping in mind the importance of data for the economy and society, as well as the circumstance that data volumes are growing and technological changes are increasing, and that, consequently, enabling free movement of data is, of course on legitimate basis, of utmost importance at both local and regional/international level;

V. Establishing and regularly reviewing joint strategy for the purpose of further development of data protection environment at the regional level, including in particular any cross-border/boundary data processing/transfer issues, all for the purpose of addressing and reducing/eliminating any potential obstacles for further improvement of mutual cooperation.

30 Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

APPENDIX I

LIST OF THE CONTACTED AUTHORITIES AND ENGAGED DATA PROTECTION EXPERTS

For the purpose of preparing and finalising this report, we have contacted the following authorities (and relevant contact persons in the respective authorities) in each of the WB economies covered by this report and the Data Protection Alignment Project:

	Authority/-ies	Contact Person/-s
Albania	Data Protection Authority (Commissioner)	Mr. Emirjon Marku, Director
Bosnia and Herzegovina	Data Protection Authority (Agency)	Dr. Dragoljub Reljić, Director
Kosovo*	Data Protection Authority (Agency) Ministry of Internal Affairs and Public Administration	Mr. Bujar Sadiku, General Director Mr. Naim Shala
Montenegro	Data Protection Authority (Agency) Ministry of Interior	Mr. Muhamed Gjokaj Ms. Zora Čizmović
Republic of North Macedonia	Data Protection Authority (Agency) Ministry of Justice	Mr. Igor Kuzevski Ms. Tanja Vasić Bozadžieva
Serbia	Ministry of Trade, Tourism and Telecommunications Data Protection Authority (Commissioner) Ministry of Justice	Mr. Milan Dobrijević Prof. Dr. Saša Gajin

The data protection experts engaged for preparing and drafting this report and communicating with the relevant local authorities as outlined above are the following:

Data Protection Lawyers in the WB Economies	International Expert
Ms. Sanja Spasenović*, ***Karanović & Partners*** *In cooperation with Karanović & Partners	Mr. Urmas Kukk
Ms. Amina Đugum*, ***Karanović & Partners*** *In cooperation with Karanović & Partners	
Mr. Veton Qoku*, ***Karanović & Partners*** *In cooperation with Karanović & Partners	
Ms. Anisa Rrumbullaku, ***CR Partners***	
Mr. Goran Radošević*, ***Karanović & Partners*** *In cooperation with Karanović & Partners	
Ms. Ljupka Noveska Andonova*, ***Karanović & Partners*** *In cooperation with Karanović & Partners	

good.better.regional.

Regional Cooperation Council Secretariat

Trg Bosne I Hercegovine 1/V

71000 Sarajevo, Bosnia and Herzegovina

T: + 387 33 561 700

www.rcc.int

@rccint RegionalCooperationCouncil RCCSec

regionalcooperationcouncil_rcc Regional Cooperation Council