Project implemented by Human Dynamics in association with:
IPS Institute
AlmavivA S.p.A.
Czech Office for Personal Data Protection OPDP
Privacy International

Project office:
Directorate for Personal Data Protection
ul.Samoilova nr.10, 1000 Skopje
Tel: (+389) 2 3230 635

Document 1.1.2 -8

ANALYSIS OF THE NATIONAL BANKING LEGISLATION FROM THE ASPECT OF PERSONAL DATA PROTECTION

Components 1

Activity 1.1.2

Document 1.1.2-8

Final version

The content of this report is the sole responsibility of Human Dynamics and can in no way be taken to reflect the views of the European Union

Support to the Directorate for Personal Data Protection

This project is funded by the European Union

Contents

I. INTRODUCTION

1. INTRODUCTORY REMARKS ON THE BANKING SECTOR REGULATION

It is fair to say that banking sector is one of the most regulated sectors in the country and worldwide. Banks and other financial institutions provide services that involve financial transactions; they have on disposal the money of the citizens and legal entities. Therefore, it is of utmost importance to set up rules that the banks and financial institutions will follow. Clients, being citizens or legal entities, must be protected, but also they need to have trust in the banks. If there is no trust and money is not placed in the bank, than that might cause severe consequences, such as increased cash transitions and gray economy and no economic growth because the investors would not be able to obtain credit. Unfortunately, this scenario occurred in the country at the end of the last century, when due to the so called pyramid savings schemes organized by several savings houses, citizens were deceived and lost a lot of funds that were deposit.

On the other hand, banks should be also safe in the relations with clients who use their services. They must prevent or limit the possibilities their services to be used for conducting illegal transactions such as money laundering and financing of terrorism, as well as other possible abuses.

All these entails clear set of rules to be established and mechanisms for supervision of their implementation. The basic rules are usually laid down in laws. However, due to the necessity to further regulate certain aspects and to adapt these aspects to the practical needs, there are also numerous bylaws, either adopted by the responsible line ministry or by the central bank as a regulatory and supervisory body in this field.

As of the reasons stated above, the rules in this sector are stricter and this can be easily noticed in the processing of personal data. As a manner of precaution, but also to satisfy the requirements of some state bodies, the banks usually process more than just basic data. Besides identifying the client and for that purpose requesting identification documents to be presented or provided, they also process data referring to the financial standing and transactions of the clients.

2. EU REGULATORY FRAMEWORK RELATING TO BANKING SECTOR

There are two EU legal acts directly relevant to the banking sector:

- **Directive 2006/48/EC** of the European Parliament and of the Council of 14 June 2006 **relating to the taking up and pursuit of the business of credit institutions**
- **Directive 2006/49/EC** of the European Parliament and of the Council of 14 June 2006 on the **capital adequacy of investment firms and credit institutions**

The aim of both directives is to harmonize the national rules of the member states in regards to the conditions and criteria to establish a credit institution (bank). They establish very precise rules on the all aspects related to founding a bank and its operations, including the possibilities of establishing branches in other member states, corporate governance issues, risk management, supervision, etc. However, there is very little in these directives that relates to personal data processing.

There is a special section in the Directive 2006/48/EC (Articles 44-52) where the rules on exchange of information and professional secrecy are set up. In short, all persons working for or engaged by competent authorities are bound by the obligation of professional secrecy. This means that any confidential information that they may receive in the course of their duties must not be divulged to any person or authority. These articles also provide clear list of exceptions where the obligation of keeping professional secret and confidentiality does not apply. Furthermore, competent authorities of the various member states may exchange information among each other. Any use or disclosure of confidential information is limited to the cases stipulated in the Directive. These provisions are transposed in Law on National Bank and Banking Law, and are further elaborated in the report.

There are two other EU directives relevant for this analysis, because they regulate certain aspects of the operations of the credit and financial institutions:

- **Directive 2008/48/EC** of the European Parliament and of the Council of 23 April 2008 **on credit agreements for consumers and repealing Council Directive 87/102/EEC**
- **Directive 2005/60/EC** of the European Parliament and of the Council of 26 October 2005 **on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing** (amended several times)

Both are transposed in two national laws, which were also analyzed for the purposes of this report.

3. BANKING LEGISLATION OF THE COUNTRY

Legislation relating to the banking sector is not codified in a single legal act. There are several laws that govern the establishment and operations of the National Bank, commercial banks and other financial institutions. Most of these laws are enacted and amended in the last several years.

After reviewing numerous legal acts that comprise the national banking legislation, the following pieces of legislation were identified as relevant and contain provisions relating to personal data processing:

- **Law on National Bank** („Official Gazette" no. 158/2010).
- **Banking Law** („Official Gazette " no. 67/07, 90/09, 67/10)
- **Law on Payment Operations** („Official Gazette " no. 113/07, 22/08, 159/08, 133/09, 145/10, 35/11)
- **Law on Foreign Exchange Operations** („Official Gazette " no. 34/01, 49/01, 103/01, 54/02, 51/03, 81/0824/11, 135/11)
- **Law on Credit Bureau** („Official Gazette " no. 81/2008, 24/11)
- **Law on Protection of Consumers in Consumer Loans Contracts** („Official Gazette " no. 51/2011)
- **Law on Money Laundering Prevention and Other Criminal Proceeds and Financing Terrorism** („Official Gazette" no. 4/08, 57/10, 35/11)
- **Rulebook on the method of reporting, registering, as well as the form, content and the method of running the Registry of direct investments of residents abroad** („Official Gazette" no.122/08)
- **Rulebook on the method of reporting, registering, as well as the form, content and the method of maintaining the Registry of non-resident's direct investments in the country** („Official Gazette" no. 122/08)

- **Rulebook on the method of reporting, registering, as well as the form, content and the method of maintaining the Registry of the investments in real estate of residents abroad** („Official Gazette“ no.72/03)
- **Rulebook on the method of reporting, registering, as well as the form, content and method of running the Registry of investments in real estate of non-residents in the country** (Ministry of Finance „Official Gazette“ no.72/03)
- **Rulebook on Operations of the Macedonian Credit Bureau** („Official Gazette“ no. 7/10)
- **Rulebook on content and form of the data that entities submit to the Office for Prevention of Money Laundering and Financing Terrorism** („Official Gazette“ no. 140/10)
- **Decision on the contents and the manner of functioning of the Credit Registry** („Official Gazette“ no.126/11)
- **Decision on manner and the procedure for opening and closing transaction account** („Official Gazette“ no.150/07, 5/08, 152/08)
- **Decision on the manner of keeping and content of the Single Registry of Accountholders** („Official Gazette“ no.146/07)
- **Decision on the bank’s information system security** („Official Gazette“ no.31/08, 78/08, 31/09)

4. USEFUL INFORMATION RELATING TO THE BANKING SECTOR

National legislation in the banking sector is primarily designed to regulate founding and manner of operating of the following entities:

- National Bank of the country (hereinafter: NBRM or National Bank)
- Commercial banks
- Other entities that run similar financial operations such as the savings houses

National Bank is the regulatory and supervisory body in the banking sector. Most of the regulations that refer to various aspects of the banking operations are adopted by the Council or the Governor

of NBRM. The most important department within NBRM in terms of overseeing the arrangements, strategies, processes and mechanisms implemented by the banks is the Supervision Department.

At this moment, there are 17 commercial banks in the country. Almost all of them are established as local banks (regardless of the fact that majority, especially the biggest ones have foreign owners), while only one operates as branch of foreign bank. In addition, there are several savings houses, micro-credit institutions, exchange offices, also referred as financial institutions. There is none electronic money issuer registered yet. All these entities collect and/or process data on their clients, who may be legal and physical domestic or foreign persons. Therefore, according to the Law on Personal Data Protection (hereinafter: LPDP), the banks and other financial institutions are considered to be data controllers and data processors. This means that they need to follow and implement the personal data protection rules set in LPDP and the bylaws based on this law, but also personal data processing related provisions laid down in the laws and regulations that govern their operations.

II. ANALYSIS OF PERSONAL DATA RELATED PROVISIONS CONTAINED IN THE BANKING SECTOR LAWS AND REGULATIONS

1. LAW ON NATIONAL BANK

Confidential information and confidentiality

There are numerous provisions in this law that speak about confidential information or confidentiality. Either some documents and reports of NBRM are treated as confidential or NBRM employees/bodies or institutions with whom NBRM cooperates must respect the confidentiality rules and principles. Most of these provisions make reference to the application of rules and regulations on protection of classified information (e.g. article 34 stipulates "*supervisory report shall be considered classified information with respective confidentiality level as specified by the regulations for protection of classified information*"). That is entirely different legislation than the one on personal data protection and another state authority is responsible for its implementation. In addition, Article 74 sets up precise rules what the confidentially in terms of NBRM operations and employees means.

Article 74

(1) No person who serve or have served as a member of the National Bank Council or staff shall, except when necessary for the fulfilment of any function or duty imposed by this Law or any other law, permit access to, disclose or publicize non-public information which they have obtained in the performance of their tasks and duties or use such information, or allow such information to be used, for personal gain.

(2) By way of derogation from paragraph 1 of this Article, member of the National Bank Council or staff may disclose non-public information, in accordance with procedures established by the National Bank, only if:

1) consent is obtained of the person about whom the information relates;

2) for the fulfilment of a duty to disclose as imposed by law, or on the order of a court;

3) given to the external auditors of the National Bank;

4) given to regulatory and supervisory authorities in the performance of their official duties; or

5) the interest of the National Bank itself in legal proceedings requires disclosure.

(3) The National Bank Council shall determine the classification and accessibility of documents held by or drawn up by the National Bank in accordance with the regulation for accessibility and protection of classified information.

The Law also provides a right to NBRM to exchange the confidential data with other domestic or foreign institutions under the conditions stipulated in the law.

Many laws in other sectors have basic rules on confidentiality and for that purpose they also refer to the application of legislation on protection rules on confidentiality and/or classified information. Making reference to the confidentiality rules is not a wrong approach, having in mind that this law mostly regulates relations between legal entities (G2B or B2B). But it would be wrong approach in cases where reference to the classified information rules is made, because classified information is produced only by government in case of national security or public safety. However, it is not excluded that in the process of exchange of all these information, there might be personal data processed as well. To conclude, it would be good, but not so necessary, if there as an additional provision or reference in the law to the adequate application of personal data processing rules.

Processing of information/data

Article 35 of the Law mandates NBRM to collect, process, analyze, abstract and disclose statistics and information relevant to the carrying out of its tasks. It also clearly requires that NBRM for that purpose shall prescribe the natural and legal persons that will be obliged to provide data, the type of data to be collected and that it may cooperate with other domestic public institutions or foreign financial institutions for that purpose.

The subsequent articles go bit further in regulating this matter by prescribing the obligation to the entities to provide information to NBRM and provide legal basis for NBRM to determine the manner, the form and the deadlines for submission of statistics and information. These articles on one hand aim to make NBRM more transparent with the information they process and on the other hand to restrict the disclosure of confidential information.

There are also few other provisions in the law where the obligation to exchange information/data with other institutions is set. In most of these provisions the type of data to be exchanged is not specified, but taken into consideration the context where they are put, it can be easily noticed that

such information is of business nature (e.g. 38 para.1 "*in pursuance of its objective to contribute to maintenance of a stable, competitive and market-based financial system, National Bank shall collect relevant data from other financial supervisory authorities, public enterprises, public institutions and companies founded by the state or where the state is a dominant shareholder, on a regular base*").

Credit Registry

Article 39 establishes the NBRM's credit registry, which as any other registry contains various types of data, including data of personal nature.

Article 39

(1) The National Bank shall establish and maintain a Credit Registry in electronic form of the credit exposure of legal entities and natural persons to banks and savings houses founded in the country.

(2) Banks and savings houses shall be required to submit data and information needed for the purposes of the Credit Registry to the National Bank.

(3) The type, the manner and the deadlines for submitting the data and the information under paragraph 2 of this Article shall be prescribed by the National Bank Council.

(4) Banks and savings houses may use the data and information from the Credit Registry in a manner and under terms prescribed by the National Bank Council and shall be deemed as classified data.

(5) The information collected for the purposes of the Credit Registry shall be used only for the purpose of improving the credit quality.

Though this article contains only few provisions regarding the Credit Registry and provides legal basis for adoption of bylaw where certain aspects will be regulated into more details, yet it is interesting from the aspect of personal data protection.

Firstly, it is clearly specified that data on natural persons (bank clients, i.e. debtors) shall be entered and maintained (processed) in this registry.

Secondly, they set obligation to the creditors to provide data on the credit operations, which include personal data on their clients who are natural persons. In addition, NBRM highest body (Council) will be authorized to determine the type, the manner and the deadlines for submitting the data.

Thirdly, the data users and the purposes for which the processed data may be used are specified, thus clearly limiting the use of data by other entities and for any other purposes.

Fourthly, data in the Credit Registry is defined and treated as classified information, which is an obvious mistake, because is produced only by government in case of national security or public safety, whereas data in the Registry is not of that type.

It can be concluded that this is a good but not the best manner of regulating the personal data processing. It is an obligation set in a law, though bit vague and not complete. Data controller/processor and data users, as well as the purpose for which the data may be used, are defined, while the details relating to the type and manner of collecting the data are to be regulated in a bylaw. Data should be treated as confidential and not as classified information. It may be reinforced by adding provision that in drafting the bylaw, the personal data protection principles and rules must be followed. Eventually, basic rules on data categories which are processed, purpose and period of processing should be given in the law.

Penalties

The law provides right to NBRM to impose severe penalties in cases where the obligation to provide information or keep secrecy and confidentially is not respected by the entities obliged to do so.

2. BANKING LAW

The present Banking Law was enacted in 2007, amended twice (2008 and 2009), but also the Constitutional Court, in several occasions, abolished few provisions of this law. It can be said that this legal act is sort of a Constitution for the banks and other financial institutions. All commercial banks in the country have to primarily follow this law and regulations adopted on the basis of this law and then the other laws that regulate the establishment and operations of business entities (Company Law). It regulates the founding, operations, supervision, and termination of operations of banks and of branches of foreign banks in the country, as well as the opening and operations of branches of banks from EU member states.

In general, Banking Law does not contain many requirements to submit and process data and documents, especially those of personal nature. Mostly, such requirements in this law can be found in the articles referring to founding of a bank, i.e. data is required to identify and determine the capabilities of the founders and persons of the governing bodies. Rules that are related to data processing are quoted and commented below.

Providing data to the clients

Article 10

(1) As for a deposit of natural person, the bank shall issue a document unambiguously stating that it is a deposit of a natural person indicating their personal data.

(2) The bank shall keep records on each payment in and out of the deposit account and, at the request by the client, issue document recording all payments in and out in the requested period.

The purpose of mandatory issuance of these two documents, both contain personal data, is to prove that transaction was made and to provide up-to-date financial information to the client. Secrecy and privacy of data contained in these documents is ensured by clearly setting the restriction on the persons to whom these documents can be issued – only to the client (at client's request).

Mandatory submission of personal data in the founding process

Article 17

(1) Persons who intend to found a bank shall submit an application to the National Bank for issuing a license for founding and operating a bank. The application for issuing a license shall comprise the following documents, data and information:

…

7. identity of the persons who intend to found a bank and the number of shares held by each of them,

8. evidence for the financial standing of the persons who intend to found a bank,

9. identity, education, experience and professional background of the nominated members of the Supervisory Board and the Board of Directors, …

Article 19

The temporary license shall include the requirements to be met by the bank in order to obtain a founding and operating license, as follows:

…

3. list of nominees with special rights and responsibilities, other than for the members of the Supervisory Board and the Board of Directors, including information on their identity, education, experience and professional background, …

Article 20

…

(5) The decision on granting a founding and operating license under paragraph 2 of this Article shall contain:

…

2. name, surname and address of natural persons, i.e. name and head office of legal entities that subscribed and paid-in shares, including the nominal amount and the number of subscribed and paid-in shares, …

Article 47

…

(2) Regarding the obtaining of license to open and operate a branch, the foreign bank shall submit an application to the National Bank, enclosing the following:

…

5. data on the members of the foreign bank's management and supervisory bodies and on identity, professional experience and qualifications (education) of the persons nominated to manage the branch, ...

These four articles specify the documents and data that banks (domestic and foreign) need to submit in order to obtain operating license from NBRM and data contained in the license issued by NBRM. Basically, there are three groups of requirements for provision of personal data: 1) identification data of founders, 2) identification data and information on their education and qualifications of the members of the bank's governing bodies and 3) identification data of founders written in the NBRM's decision for granting a license. The law does not require more than it is really necessary to identify the persons who are either founders or managers (name and address). Additional requirements to provide information on the educational and professional background of the managers and the financial standing of the founders are understandable, because it is a highly regulated market and profession. In addition, there are several provisions in the law that refer to the persons with special rights and responsibilities in the bank or branch, and that in some cases data referring to them should be publicly available. Past experiences in the country and worldwide have shown that abuses made from these persons cause negative financial consequences to many citizens and country's economy in general. So, requirement to submit or to publish these data can contribute in timely prevention of such abuses. It can be concluded that public interests prevail over private interests. Though, there is no much personal data required to be revealed.

Officers and units with auditing and compliance role

This law introduces and regulates two special positions or units within the banks. **Internal Audit Department** must be established and operate as an independent organizational unit in each bank (Article 95). The Internal Audit Department is mandated to conduct constant and full-scope audit of the legitimacy, accuracy and promptness of the bank's operations assessments of the implementation of the bank's policies, procedures, information systems, etc. Each bank must also appoint **Compliance Officer** or organize a **Compliance Department** (Article 99). The officer/department is mandated to identify and monitor the risks arising from the non-compliance of the bank's operations with the regulations. Both departments shall be specialized to perform solely the activities within the scope of work defined in the law and shall be independent in performance of the activities.

The reason why these internal positions/bodies are mentioned here is because of their similarity with the **Personal Data Protection Officer**, who according to the LPDP must be appointed in each personal data controller and processor. The provisions in LPDP also require this officer to be highly ranked in the organization's hierarchy and to be independent from others. Most of the assessments the Internal Audit Department does overlap with the assessments and controls carried out by the Personal Data Protection Officer. As of that reason, it would be good solution if departments at the same time act as personal data protection officers/units. However, banks are large entities that due to the complexity of the work and huge number of persons they employ could establish separate and independent unit for personal data protection, which in such case must closely coordinate its work with the Internal Audit.

Exchange of data with NBRM

Article 101

(1) The banks shall submit reports and data to the National Bank.

(2) The National Bank Council shall prescribe in more details the forms, types, methodology, contents of the reports and data, and the deadlines for their submission to the National Bank.

(3) The National Bank Council may prescribe reports and data which are to be published by the bank, as well as the manner, the form and the deadlines for their publishing.

It is up to the NBRM to decide the type of data that it will collect from the banks. Mostly, it will be statistical data or data of business nature. However, in some cases it might be a personal data, like in the case of the Credit Registry. Therefore, categories of data should be clearly stipulated by law. These decisions of NBRM are elaborated in the other sections of this report.

Bank secrecy

Article 111

Any documents, data and information acquired through banking and other financial activities on individual entities, and transactions with individual entities and on deposits of individual entities shall be considered bank secrecy the bank is required to protect and keep.

Article 112

(1) Persons with special rights and responsibilities, shareholders and bank employees, who have access to the documents, data and information from Article 111 of this Law, as well as other persons who, by rendering services to the bank, have an access to the documents, data and information referred to in Article 111 of this Law, shall keep them, and may use them only for the purposes they were obtained for, and shall not disclose them to third parties.

(2) The requirement under paragraph 1 of this Article shall not be applied in the following instances:

1) if the data and information disclosure is prescribed by a law, and

2) if the person gave a written consent to data disclosure.

(3) For the persons with special rights and responsibilities, and bank employees, the requirement under paragraph 1 of this Article shall not apply also in the following instances:

1. on written request of a competent court for conducting procedures within its competencies,

2. for the needs of the National Bank or another supervisory body authorized by law,

3. on written request of the Public Revenue Office for conducting procedures within its competencies,

4. if the data are disclosed to the Anti-Money Laundering and Combating the Financing of Terrorism Office, in accordance with the law,

5. if the data are disclosed to the Financial Police Office, in accordance with the law,

6. on written request of the State Foreign Exchange Inspectorate for foreign exchange operations control,

7. on written request of the Deposit Insurance Fund, in accordance with the law,

8. if the data are disclosed for the needs of operating the National Bank Credit Registry and to the credit bureau, in accordance with the law, and

9. on written request of the enforcement agents in accordance with the law.

(4) The persons who, in accordance with paragraph 3 of this Article, obtained the documents, data and information referred to in Article 111 of this Law, shall keep them, may use them only for the purpose they were obtained for, and shall not disclose them to third parties, unless in cases and procedure stipulated by this or another law.

(5) The requirement under paragraphs 1 and 4 of this Article shall continue being valid after the termination of the employment, i.e. after the termination of the ground and the status underlying the access to the data regarded as bank secrecy.

These are very important provisions, which actually refer to the personal data and privacy of the banks' clients in a broader sense. It is clear that all the data and documents provided to the bank and transactions made by the clients are deemed as secret and that as such must be treated by all banks' bodies and employees. The exceptions are clearly specified and are in compliance with the other laws that require data to be provided to certain state institutions mostly for investigation purposes.

Article 171

(1) The banks shall act pursuant to the regulations on anti-money laundering and combating the financing of terrorism.

(2) The National Bank shall conduct supervision on AML/CFT systems in the bank.

Only two provisions refer to this worldwide important issue - anti-money laundering and combating the financing of terrorism. The reason for this is that there is special law that contains detailed rules on this matter. So, in order to avoid repeating and overlapping, the approach of the Banking Law is to make a reference to this law. In addition, the Banking Law delegates the authority to NBRM to supervise the AML/CFT systems and procedures in the banks. There is a special part in this report where the Law on Anti-Money Laundering and Financing Terrorism is analyzed.

3. DECISION ON THE BANK'S INFORMATION SYSTEM SECURITY

This Decision of NBRM is adopted in 2008 and amended twice since then. Rules laid down in this decision shall be applied by all commercial banks and savings houses. According to the Decision, they must establish and implement IT management system and security policies and procedures. More precisely, the Decision sets forth the methodology for security of the bank's information system, establishes standards for the information system security through defining criteria for establishing process for managing the information system security, ensuring business continuity, as well as security standards for the e-banking systems and the bank's outsourcing companies. Banks are required to establish a system for identification, measurement, monitoring and control of the information systems incompatibility risk.

Each bank is obliged to adopt and implement Information System Security Policy, where the process of managing the information system security risks shall be defined. Among other issues, this Policy shall include "*rules on protection of personal data, in conformity with the enforced regulations in the country".* Other elements that shall be included in the Policy are basically the standard organizational and technical measures, which to some extant are already given in the Decision, including the division of roles and responsibilities, risk management, etc.

4. CREDITS AND LOANS

a) LAW ON CREDIT BUREAU

The Law on Credit Bureau was enacted in 2008 and amended once in 2011 (to modify the penalty provisions). **Goal of this law is to regulate the establishment and operations of the credit bureau, processing of data, the type of data and the manner of its submission to the credit bureau**. Though singular form (bureau, not bureaus) is used in the law, the aim is not to create a monopolistic market, but to allow to any company established as joint stock to fully or partially collect and process data about data subjects in order to provide accurate reports on the financial obligations and on the regular payments of these obligations by the data subjects. Credit bureaus, if established, should contribute to better and coordinated assessment of the legal and natural persons' payment capabilities and in reducing the risks relating to credits and other financial obligations.

By reading the article 1 of this Law it becomes clear that **the law is tightly related to the Law on Personal Data Protection**. The link is established in article 3, paragraph 3, where the reference to the LPDP provisions is made ("*for the use of data and reports referred to in this law provisions of LPDP shall be adequately applied*"). The same provision adds that LDPD is *lex generalis*, by giving priority to the provisions of the Law on Credit Bureau ("*LPDP provisions shall adequately apply unless this law stipulates otherwise"*).

Article 5 sets up the **basic data protection principles and obligations**:

"(1) The Credit Bureau shall perform the activities impartially and shall ensure the privacy of the data subject.

(2) The Credit Bureau shall regulate its operations with an act which is published in Official Gazette and on its website.

(3) The act under paragraph 2 of this Article shall be approved by the Directorate for Personal Data Protection in the part concerning the protection of personal data."

Provisions from Article 8 have similar content. They impose obligation to the credit bureau to define into more details the rules and **principles on confidentiality, accuracy, relevancy and use of data** and obligation to establish and implement **organizational, technical and administrative measures**. DPDP must give approval to the established measures, which is in line with the LPDP and the Rulebook on Organizational and Technical Measures for Providing Secrecy and Protection of Personal Data Processing.

According to Article 15, **credit bureau must adopt an internal act on the manner of exchange of data with the data provider**, for which the Directorate must give prior approval. Since the transfer of data from the data provider to the credit bureau and from the credit bureau to the data user (Article 18) will be carried out in electronic form, the provisions prescribe that the data must be encrypted and secure line used. Although other technical measures should be prescribed and implemented, this can be done in the internal acts which will anyway be reviewed by DPDP.

All these, sort of safeguard, clauses prevent the companies registered as credit bureau to operate without prior adoption of internal acts, which must be reviewed and approved by the Directorate. This actually gives additional power to the Directorate and serves as guaranty to the citizens (clients of certain financial institution) that their personal data will not be abused.

Article 9 requires **contract to be signed between the data provider and credit bureau**, which means that contractual provisions will apply in addition to the provisions from this law and the credit bureau's internal acts.

Article 11 specifies the **data providers** (public and private entities), while article 14 specifies the **type of data that may be collected by the credit bureau**. The type of personal data that may be collected seems not to be excessive, because it is data necessary to identify the data subject (name, address, and unique citizen's number) and his payment obligations, thus making the credit bureau's provision of services possible.

Article 16 sets up the following data processing rules for the credit bureau relating to the reports it issued:

- Report containing data will be provided upon a **request**,
- Report will solely refer to the **data subject total obligations** without revealing: a) identity of the data provider and b) specific data subject obligations with the data providers.

In a way, the latter rule keeps to certain extant the privacy and secrecy of the data subjects towards third parties – data users. However, provisions referring to the report that the credit bureau issues should be based on clear distinction between a **positive and a negative credit history register**. While positive credit history register is based on data subject consent, the negative is not, which means that the data can be provided to the party that requested it without having consent of the data subjects. This is justified because it is even of the public interest to prevent possible abuses.

Additional compliance with the personal data protection rules is ensured with the provisions of article 21. Namely, if there is no **consent given by the personal data subject**, than the credit bureau cannot provide the report to the data user.

Article 19 requires that the **collected data must be kept for 5 years** from the date the data subject has paid its dues or closed the account. It seems that this is a long period of time, especially taking into consideration that the obligations have been paid and there is no justifiable reason to continue keeping the data.

Obligations for the credit bureau to provide to the data subject information on data providers and data users are contained in article 24, while the **obligation to present to the data subject his/her rights** is laid down in article 26. Among the rights of the data subjects are: right to withdraw the given consent (article 27) and right to dispute the data contained in the register and/or report (articles 28-32). The obligation to provide accurate and up-to-date data and to correct the data upon a request of the data subject has to be followed by the data provider as well. All these rights are in compliance with the provisions of LPDP relating to the rights of the data subject.

Article 42 stipulates that personal data processing shall be conducted in accordance to the **organizational, technical and administrative measures** and that each data stakeholder (credit bureau, data providers and data users) must prescribe and implement such measures. It is good that this article clearly requires personal data protection rules to be followed when establishing the measures.

It is questionable whether is the right solution to **transfer the entire data and documents to the State Archive Office once the credit bureau ceases to operate, who should keep them for 5 years** (Article 45). The data that credit bureau collects is not of archive nature and the credit bureau itself is a private entity, not a public institution. Moreover, the Archive keeps the archive documents permanently. If there is a need to transfer the data, than it should be to another state entity (e.g. NBRM), though it seems that the best solution would be to completely destroy the data.

The law gives **surveillance authorities** to DPDP and it contains penalties that may be imposed if the obligations have not been observed by the entities that provide, process or use personal data.

Based on this Law, in 2010 **Macedonian Credit Bureau (MCB)** was founded by KIBS (Clearing House). Ac required by the law, MCB adopted internal acts that contain rules on various aspects relating to its operations. The highest internal act is the **Rulebook on Operations of MCB**. It has a separate chapter on the manner of data processing, though the more technical aspects are regulated in other

acts. Article 52 is dedicated to the protection of personal data; where reference is made to and compliance is ensured with the legislation on data protection. The initial versions of this Rulebook, as well as of the other internal acts were not approved by DPDP due to their incompliance with the personal data processing rules and principles. However, this Rulebook and the other internal acts that are now in force are without any doubt compliant with LPDP. Furthermore, Article 52 paragraph (3) stipulates "*if the data is wrong or there is no longer need to keep the data in the register, it shall be deleted*". This is a much better solution and right approach than the provision of similar character contained in the law.

The only issue that might be reconsidered and modified by MCB is related to the **manner of keeping the dossier for each data subject**. Namely, for the data subject who is a natural person his/her unique citizen's number shall be used to identify him in the system and to keep the dossier. Use of this special category of data should be restricted as much as possible. It is reasonable to collect this data, because it uniquely identifies the data subject, but there should be another method used (random numbers or characters) to identify and categorize the data subject in the MCB system. Furthermore, processing and use of PIN cannot be set in a bylaw.

b) CREDIT REGISTRY OF NBRM

Article 39 of the Law on NBRM establishes the NBRM's Credit Registry, but the detailed rules are to be found in the **Decision on the contents and the manner of functioning of the Credit Registry**, which was adopted by the Council of NBRM in 2011. The Credit Registry of NBRM is a collection of personal data, controlled by NBRM. The aim of the Credit Registry is to enable:

- centralization of the data on the credit risk exposure to clients submitted by banks and savings houses;

- utilization of data and information on the credit risk exposure by the banks and savings houses for the credit risk management purposes;

- provision of data and information on the credit risk exposure of individual bank and savings house for the purposes of the supervisory function of NBRM.

The **type of data collected** for purposes stated above is mostly of personal nature. It is data necessary to identify the data subject (name, address, and unique citizen's number - PIN) and its payment obligations. This Decision provides to the **data subjects right** to enclose evidence to the bank or savings house that their personal data in the Credit Registry are incomplete, inaccurate, or

not updated and upon their written request, the bank or savings house shall be required to supplement, or modify data, to delete them and to replace them simultaneously with accurate data, or to terminate the use of incomplete, inaccurate, or not updated data, simultaneously replacing them with accurate ones. It is not clear why this provision will enter into force and the right may be exercised as of March 2012. Article 10 specifies and limits the **type of data that may be provided to the Credit Registry users**. Although there is legal basis in 39 to regulate in the bylaw the type of data to be processed, yet it is a matter that should be prescribed in the law. Moreover, rights of data subject in relation to its personal data must be always prescribed in a law.

Basic requirements relating to the use of this electronic system can be found in Article 9. Namely, the person/entity accessing the Credit Registry data and information must be authenticated, while the access to be authorized and recorded. These provisions are in line with the personal data processing principles which require technical measures to be implemented for the information systems (secure authentication method and only for authorized users).

This Decision makes the same mistake as many other laws do in terms of not making reference only to the legislation on classified information (*Art.9 "the Credit Registry data and information shall constitute classified information on the banks, savings houses and foreign bank's branch office"*), which are different set of rules than the personal data processing rules. As it is clear that personal data is being processed through the register and electronic system, **the correct reference should be to the personal data protection rules.**

Based on this decision, NBRM has developed **Instructions that lay down the manner and the timeframes for submission and utilization of data and information in the Credit Registry**. There are two ways to use the data from the Credit Registry: through the special web application (intranet environment with restricted access to the computer network and database) and web services. These instructions do not provide more technical and organizational measures for protection of the data, though act of this nature should have such provisions.

c) LAW ON PROTECTION OF CONSUMERS IN CONSUMERS' LOANS CONTRACTS

The present Law on Protection of Consumers in Consumers' Loans Contracts was enacted in 2011. It transposes the provisions from the Directive 2008/48/EC. As stipulated in Article 1, this law regulates the protection of consumers in concluding and executing contracts for consumers' loans, to the extent and for purposes provided by this law. The key terms that the law defines are the following:

- "Consumer" means the natural person who concludes a contract for consumer loan in accordance with this law and for achieving the goals that are not connected with the performance of his trade, business or professional activity;
- "Creditor" is a bank or other company and sole proprietor that within its registered office, approves or promises to grant loan to consumers;
- "Consumer loan agreement" means an agreement approved by the creditor or promises to grant consumer loan in the form of loans, overdrafts, deferred payment of goods and services, financial leasing or other similar financial services, except contracts for the provision of services on continuous basis or for supply of products of the same kind in which payment is made in instalments during the period of provision of services and supply of products.

There are couples of articles which relate to collecting or processing of personal data, but in general the law aims to regulate some other aspects in these contractual relationships, thus protecting the consumer from possible financial abuses.

Article 8 requires from the creditor, before it concludes a contract for consumer loan, to assess the creditworthiness of the consumer on the basis of sufficient information supplied by the consumer or, if necessary from the relevant database. Though, this provision is taken from Article 8 of the Directive, there are two interesting aspects in this provision.

First, it leaves to the creditor to decide what type of information to be requested from the potential consumer. It's quite understandable that assessing creditworthiness of a person will certainly require collecting of bit more personal information than other types of assessments. Question is whether wording used "sufficient information" leaves freedom to the creditor to collect personal data from the consumer, which might not be relevant or that might be too excessive for the purposes. Therefore, this provision might be modified to avoid broad interpretations (e.g. "*creditor may collect additional data from the consumer only if it is relevant, appropriate and not excessive for the purpose of assessing the consumers' creditworthiness*".

Second, it stipulates that data on the creditworthiness of the consumer may be assessed by collecting information from a relevant database. There is no further reference on what databases may be used. However, whatever database is used for this purpose, that database will certainly be subject of other national regulations. This means that rules from other laws and bylaws will apply for the manner of use of the database, and that would be the right place to assess if personal data processing rules have been incorporated. Such, probably frequently used, database will be the Macedonian Credit Bureau's database, which rules have been analysed and presented in this Report.

Article 10 lays down the obligatory elements of the consumer's contracts. Out of all the elements and information that must be part of these contracts, only couple of them are of personal nature related to the contracting parties – name and address of the consumer and of the creditor (if the creditor is a natural person – sole proprietor). This is certainly appropriate and not excessive data that should be contained in the contract. However, the list of contractual elements ends up with "Other contractual information, if applicable". This type of phrase always gives freedom to the party that writes the contract, in this case the creditor, to add various types of information. This broad possibility given by the law might be useful in some cases in order to add and regulate some specifics, but not when it comes to personal data. It would be better, as proposed for other laws, to modify this phrase so that it reads "*other contractual information, except for personal data that is not appropriate, not relevant and to excessive for the purpose of concluding the contract*".

Article 23 delegates a task to the Ministry of Economy to establish and keep Register of Creditors of Consumer Loans and Register of Credit Intermediaries who have obtained permit to approve loans. **Rulebook on the Form, Content and Manner of Keeping of the Registry** is adopted in 2011. In this Registry data relating to the creditors are entered. This data is of business character, because the creditors are actually legal entities or registered sole proprietors, not natural persons; therefore personal data processing rules do not apply.

5. PAYMENT OPERATIONS

The present **Law on Payment Operations** was enacted in 2007 (entered into force on 1 January 2008) and it has been amended five times since then. It regulates the payment operations in the country, relations between payment operations carriers and payment operations participants, relations between payment operations carriers and NBRM concerning payment operations, payment systems, payment settlement, issuance of electronic money and oversight of payment systems.

According to Article 3 of this Law **payment operations carriers** are: NBRM, banks that were granted a license to perform payment operations, Treasury at the Ministry of Finance as a special payment operations carrier for budget users and individual users and the Treasury of the Health Insurance Fund as a special carrier of the payment operations of the health institutions. Taking into account that payment operations include opening and maintaining of accounts to the natural persons and processing of personal data for the purposes of realization of payment transactions, all these entities are data controllers, processors and users, while the natural persons - accountholders are data subjects.

Article 4 indicates the tasks/activities undertaken by the payment operations carriers, among which are the obligation to **ensure secrecy of data** on the transaction account balance and to **protect the data** on the transaction accountholder. It is a good solution to place these obligations among the main ones that payment carrier should fulfil, because it speaks about the importance to protect confidentially and privacy for these sensitive transactions.

Article 12 stipulates that the **manner and the procedure for opening and closing transaction account shall be prescribed in a Decision adopted by the Governor of NBRM**. The Decision was adopted in 2007 and amended twice since then. The most relevant provisions of this Decision are presented below.

- Article 6 of the Decision regulates the **manner of identification of the natural person by the payment operations carrier**, which must be done before the account is opened. It requires an ID card to be presented in order to determine the identity and the resident address of the accountholder. If there are other persons authorized to manage the account, then their IDs must be presented as well. Article 7 provides possibility to the payment operations carrier to determine in its internal rules that other documents may be required from the accountholder, including his/her contact details; while Article 8 stipulates that it is not sufficient only to present the ID and other documents, but payment operations carrier must also keep a copy of them. It is understandable that the accountholder must be identified, because payment operations carrier

and the accountholder conclude contract with rights and obligations that might result in dispute resolution procedure and also the contract provides to the accountholder to carry out financial transactions. But, requirements to store the documents that prove the identity of the contracting party, as well as to determine other documents and data to be provided by the accountholder are problematic. The latter requirement opens possibilities for processing and storing of other documents and personal data. Therefore, it is better to clearly specify in this Decision all the documents and personal data that may be required and eliminate possibilities for the banks to determine additional personal data and to take copies of identification documents.

- Article 10 of the Decision requires a **contract to be concluded between the payment operations carrier and the accountholder** and it sets the mandatory elements of the contract. Since the content of the contract is not limited, the payment operations carriers may add in the contracts additional data, including personal data, which it seems to be the case in the practice. As in the previous case with the documents required to be submitted by the accountholder, it would be good to add provision in this Decision that "personal data other the one stipulated in this Decision cannot be required and contained in the contracts" or that "contract shall contain only personal data that is appropriate, relevant and not excessive in relation to the purposes for which they are collected and processed."

Article 15 establishes the **Single Registry of Accountholders**, while article 16 prescribes that data from this registry may be used under the terms stipulated by this and other law. Based on these provisions, **Decision on the manner of keeping and content of the Single Registry of Accountholders** is adopted by NBRM in 2007. Article 2 of the Decision specifies the mandatory data that must be provided to and kept in the Register, such as the name and the address of the natural person – accountholder, as well as the conditionally mandatory data such as the Unique Citizen's Number and contact data of the accountholder. As these data are already required for opening of an account, than their entering into the Single Registry seems appropriate and necessary in order to identify the person in the Registry and for seamless carrying out of transactions that involve different payment operations carriers. However, it should be further assessed if it is possible to have a centralized register of accounts, not of accountholders. In such case, only the account number and a bank which administers this account will be entered in the Registry.

Special chapter in this Law is dedicated to the **electronic money**, with emphasis on the entities that may provide this service. Conditions to become e-money issuers can be met by banks or companies that have strong IT infrastructure and security policies in place, which also have greater interest.

Therefore, it is clear why article 38 allows to the e-money issuers to perform data storage on electronic devices on behalf of other legal entities as an additional service.

The Law also dedicates special chapter on **keeping documents**. Article 49 prescribes that payment operation carrier shall keep the payment instruments and other documents underlying the recording of changes in transaction accounts at least five years after the end of the calendar year in which the changes have been registered. An additional obligation for the payment operations carrier is to keep the data from the transaction account registry permanently, while the documentation underlying the opening and closing of transaction account shall be kept for five years after the end of the year in which the transaction account has been closed. It is questionable if it is really necessary to keep payment instruments and documents which contain personal data for 5 years or this period can be shortened (are there requirements in other laws that entail to keep these records for proving purposes). Same goes for the requirement to permanently keep the data from the Single Registry of Accountholders.

6. FOREIGN EXCHANGE OPERATIONS

The present Law on Foreign Exchange Operations was enacted in 2001. It was amended six times since then, but also the Constitutional Court has abolished couple of provisions. The Law regulates: 1) current and capital transactions and their execution in form of payments and transfers among residents and non-residents, among residents if using foreign means of payment or if the subject of operations are foreign means of payment and unilateral transfers of funds from or the country which do not represent transactions among residents and non-residents, and 2) foreign exchange supervision and control.

There are no provisions in this law that directly stipulate personal data processing or that relate to privacy issues. However, there are several registries established by this Law, but the method of reporting, registering, as well as the form, content and the method of maintaining the registries shall be prescribed in bylaws adopted by responsible ministries. There are too many bylaws adopted on the basis of this law, but the following relate to the registries:

- Rulebook on the method of reporting, registering, as well as the form, content and the method of running the Registry of direct investments of residents abroad
- Rulebook on the method of reporting, registering, as well as the form, content and the method of maintaining the Registry of non-resident's direct investments in the country
- Rulebook on the method of reporting, registering, as well as the form, content and the method of maintaining the Registry of the investments in real estate of residents abroad
- Rulebook on the method of reporting, registering, as well as the form, content and method of running the Registry of investments in real estate of non-residents in the country

The first two rulebooks are adopted by the Ministry of Economy in 2008, while the latter two by the Ministry of Finance in 2003. They all contain templates for registration of specific investment. Personal data that should be entered in this registration form is the basic data to identify the person: name, address and Personal Identification Number of the person. This seems to be appropriate personal data and relevant for the purpose it is requested. In addition to the request to enter this data in the registration form, it is mandatory to enclose a copy of the identification document. Besides the personal data, it is also required to enter data related to the specific type of investment, which should be used for statistical purposes.

The only unnecessary data required to be entered in the registration form of non-resident investment in the country and registration form of resident investment abroad is the PIN of the authorized person to submit the application in behalf of the non-resident or the resident. It is sufficient to enter the names and contact info.

7. ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM

a) LAW ON MONEY LAUNDERING PREVENTION AND OTHER CRIMINAL PROCEEDS AND FINANCING TERRORISM

The present Law on Money Laundering Prevention and Other Criminal Proceeds and Financing Terrorism was enacted in 2008 and amended twice (2010 and 2011). It follows the Directive 2005/60/EC on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing. The Law lays down the measures and actions for detection and prevention of money laundering and other criminal proceeds and financing terrorism. Money laundering and financing terrorism activities are crimes as defined in the Criminal Code.

Measures and actions for detection and prevention of money laundering and financing terrorism to great extent restrict the privacy. However, it is a global issue that the country had to follow by adopting this law and taking concrete actions to prevent or fight against these crimes. So, the question if this law and the prescribed measures and actions are necessary is obsolete. Apparently, it must be present and applied, regardless of the fact that interferes into citizen's private life. Therefore, the review of this law was more focused on the authorizations, time periods, security measures, etc. It can be freely said that the entire law is closely related to privacy in broader sense. However, only the articles that in my opinion are the most relevant from the aspect of personal data processing are presented below, with personal comments added bellow each article.

Article 3

(1) An Office for Money Laundering Prevention and Financing Terrorism (hereinafter referred to as: the Office) shall be established for collecting, processing, analysing, keeping and providing data obtained from the entities which are bound to undertake measures and actions for detection and prevention of money laundering and financing terrorism, as a body within the Ministry of Finance in the capacity of a legal person

(2) The Office shall have the following competences:

- to seek, collect, process, analyse, keep and provide data obtained from the entities on the basis of this Law,

- to collect financial, administrative and other data and information necessary for the performance of its competences,

...

It is clear that the main task of the Office is to process data. Mostly, it is data of personal nature, though business data is also subject of scrutiny of the Office. The Office is at the same time data controller, processor, provider and user. Therefore, all the personal data protection rules referred to these four categories must be applied by the Office, including the exceptions provided therein.

Article 5

Entities shall be the persons who have the obligation of undertaking measures and actions for prevention and detection of money laundering and financing terrorism provided for in this Law (hereinafter referred to as: entities), such as the following:

1. Financial institutions and subsidiaries, branch offices and business units of foreign financial institutions performing actions in the country in accordance with the regulations;

2. Legal and natural persons performing the following activities:

a) trade in real estate,

b) audit and accounting services;

c) notary public, attorney and other legal services relating to: sale and purchase of movables, real estate, partner parts or shares, trading in and management with money and securities, opening and managing bank accounts, safe-deposit boxes and financial products, establishing or taking part in the management or operation of the legal entities, representing clients in financial transactions etc.,

d) providing advices in the area of taxes;

e) providing consulting services and

f) providing services of investment advisor.

3. Companies organising games of chance in a gambling room (casino);

4. Associations of citizens and foundations (domestic and foreign);

5. Service providers to legal persons;

6. Central Securities Depositary;

7. Legal entities taking movables and real estate in pledge;

8. Agency for Real Estate Cadastre and

9. Legal entities whose activity is sale and purchase of vehicles

The list of entities that shall collect data and process it to the Office is pretty long. It is determined based on the nature of the operations that entities carry out - registering financial transactions or transactions of commodities of higher value and working with clients. All of them should apply the provisions of this law, but also the legislation on personal data processing. It is questionable if it is really necessary for the NGOs or service providers to legal persons to be included in this list.

Article 6

Measures and actions for detection and prevention of money laundering and financing terrorism (hereinafter referred to as: measures and actions), undertaken by the entities shall be the following:

- client due diligence;

- monitoring of certain transactions;

-collecting, keeping and submitting data on transactions and clients performing them, and

-introduction and application of programmes.

Article 8

The entities shall be bound to apply client due diligence procedures in the following cases:

a) when establishing a business relationship;

b) when carrying out one or several linked transactions amounting to EUR 15,000 in denar counter-value;

c) when there is suspicion of money laundering or financing terrorism, regardless of any exception or amount of funds; and

d) when there is doubt about the veracity or adequacy of the previously obtained client identification data.

These two articles clearly define how deep the entities should be in achieving the goals set by the law – preventing anti-money laundering and terrorism. They set up the type of measures to be

implemented and when should they be taken. Implementation of such measures diminishes the privacy, but it is considered to be done for legitimate and higher causes.

Article 9

(1)The customer due diligence procedure referred to in Article 8 of this Law shall include:

a) identification of the client and verification of his/her identity;

b) identification of the authoriser and verification of his/her identity and identification of the beneficial owner, his/her ownership and management structure and verification of his/her identity;

c) obtaining information on the purpose and intention of the business relationship and d) conducting ongoing monitoring on the business relationship.

(2) The entities shall apply each of the measures provided for in paragraph 1 of this Article, but they may determine the extent of such measures depending on the client's risk assessment, the business relationship, the product or the transaction.

...

It is a reasonable and necessary step to identify the client, as stipulated in paragraph 1. Provision in paragraph 2 prevents application of the same identification procedure to all clients. This provision should be read that risk assessment procedure should be the basis to determine the type of identification procedure to be applied for each client. This means that each client or groups of clients should be treated differently - if the risk is lower than the identification and due diligence should be as simple as possible.

Identification and verification of the identity of the client

Article 10

(1)When the client is a natural person, he/she shall be identified and his/her identity verified by submitting an original and valid document, personal identification card or passport or a copy of a personal identification card or passport certified by a notary public.

(2)When the client is a foreign natural person, he/she shall be identified and his/her identity confirmed on the basis of the data specified in his her original valid identification document, personal

identification card or passport or a copy of the valid identification document certified by a notary public or authorised institution in his domicile country.

(3)The document referred to in paragraphs 1 and 2 of this Article shall be used to determine the name, surname, date and place of birth, place and address of living and residence, the unique registration number or identification number and number of the ID card or passport, the issuing authority and the date of validity of the ID card or passport.

(4)If any of the data referred to in paragraph 3 of this Article cannot be determined from the identification document, personal ID card or passport, original or copy of the identification document certified by a notary public or the competent institution in the domicile country, the entity may request another public document or certified statement from the client on the demanded data and its accurateness.

(10)The entities shall obligatorily keep copies of the documents referred to in paragraphs 1, 2, 5, 7, 8 and 9.

(11)On the basis of internal acts, the entities may also request other data required for the identification and verification of the identity of the client or the beneficial owner.

Identification and verification of the identity of the beneficial owner (user)

Article 11

(1)The entity shall be obligated to verify the identity the beneficial owner and on the basis of risk analysis, to verify his/her identity in accordance with Article 10 of this Law.

(2)When the entity cannot identify the beneficial owner according to paragraph 1 of this Article, it shall take a statement from the client, and it shall verify the identity on the basis of data from independent and reliable sources.

Identification and verification of the identity of the authoriser

Article 12

(1)If the transaction is carried out in the name of and on the behalf of a third party, the entities, in the cases when the law stipulates such an obligation, shall be bound to establish and verify the identity of the person performing such a transaction (authorized person), the holder of the rights, the client acts (the authoriser) and the authorization.

(2) If it is not certain whether the client acts on his/her own behalf and account or on behalf and for the account of a third party, the entity shall be bound to request information from the client for

determining the identity of the holder of rights (the principal) and the power of attorney i.e. the certified contract between the principal and the proxy.

These three articles establish the manner of identification of three types of persons: clients, beneficial owners and authorisers. ID cards or passports are the primary documents to be used for identification purposes. Basically, all the data in the identification documents should be checked by the entities (employees) and in addition copy of the documents to be kept by the entities. It is questionable if the requirement to keep a copy of the identification document serves any purpose, because on one hand it is not a 100% certain evidence and on the other hand it might be more easily abused.

Ongoing monitoring on the business relationship

Article 12-b

(1) The entities shall be obliged to monitor the transactions performed within the framework of the business relationship with the client, with a view to confirming that those transactions are carried out according to the purpose and intention of the business relationship, the risk profile of the client, the client's financial situation and if necessary the client's financing sources.

(2) The entities shall be obligated to regularly update the documents and the data about the client, collected during the implementation of the activities referred to in Article 9 paragraph 1 items a), b) and c) of this Law.

These provisions make the entities' role similar to the one of the law enforcement agencies, because the client transactions should be monitored permanently and client's personal data and identification documents to be regularly updated in the entities' data collections.

Article 12-d

(1) Financial institutions shall be bound to provide data on the instructing party including: name and surname, i.e. name of the instructing party, address and account number upon the payment of an amount exceeding EUR 1000 in denar counter value according to the median exchange rate of the National Bank on the day of the payment for the purposes of cashless transfer through the international payment operations. If the data on the address is missing or cannot be determined, the

financial institution may replace it with: the date and place of birth or the personal identification number of the client or identification, i.e. referent number of the client.

(2) Financial institutions shall be bound to provide data from paragraph 1 of this Article upon the payment of an amount exceeding EUR 1000 in denar counter value according to the median exchange rate of the National Bank on the day of the payment for the purposes of cashless transfer through the domestic payment operations. If due to technical reasons, the provided data cannot be forwarded, only the data in the account number or the unique identification number shall be forwarded.

(3) On the request of the financial institution which should made the payment, or the competent authorities, the financial institutions from paragraph 2 of this Article shall be bound to make them available three working days at the latest starting from the delivery of the request.

(4) On the day of the transfer in the international payment operations the financial institutions occurring as mediators in the cashless transfer for the amounts exceeding EUR 1000 in denar counter value according to the median exchange rate of the National Bank are bound to forward the data on the instructing party from paragraph 1 of this Article to the financial institution which will perform the payment of the transfer.

(5) Upon payments of cashless transfers in the amount exceeding EUR 1000 in denar counter value according to the median exchange rate of the country on the day of the payment, the financial institutions shall be bound to determine the manner by which they will determine whether part of the data from paragraph 1, 2 and 4 of this Article are missing, as well as the manner of proceeding with such transfers within the frames of their internal acts. The entities should demand the missing data or refuse the performance of the transfer.

In addition to the general obligations provided in this law, the above cited article and articles 19-23 stipulate specific obligations for the entities in various sectors to collect and process personal data relating to transactions exceeding certain amounts. These obligations refer to the financial institutions, Customs Office, entities performing exchange operations, providers of fast money transfer, organisers of games of chance in gambling room (casino) and brokerage firms and banks licensed to operate with securities. The amount for which they are obliged to identify the client (collect data) differs and depends on the sector. There is also an additional provision that applies to the Customs Office and it refers to the manner of reporting to the Office. Namely, the reporting should be conducted in electronic manner or by telecommunication means (telephone, fax), and where this is not possible, by other means in writing.

All these entities are obliged to keep the records for certain period of time (Article 27). The bookkeeping periods for all entities are 10 years, but the commencement date of the period for each entity differs. The entities are also bound to make available the identification documents on a request of the Office or the surveillance bodies.

Submission of data to the office

Article 29

(1)The entities shall be bound to submit to the Office the data collected, the information and the documents to the Office in the following cases:

(a) when there is suspicion or there are grounds for suspicion that money laundering or financing terrorism has been performed or an attempt has been made or is being made for money laundering or financing terrorism,

(b) in case of cash transaction in the amount of EUR 15,000 in denar countervalue or more,

(c) in case of several connected cash transactions in the amount of EUR 15,000 in denar counter-value or more.

Entities are obliged to collect data, but not each data is further processed to the Office. Only if one of the above stated conditions is met, than submitting data to the Office is mandatory. In addition to this general obligation, for some specific entities there is obligation to submit data to the Office in other cases as well. If there is any transaction exceeding 15.000 Euros which involve entities such as: public notaries, banks, insurance companies and legal and natural persons whose business activity is buying and selling of vehicles, than the entity must report the transaction to the Office. Article 31 lays down the manner of submission of data to the Office. Electronic form or telecommunication means (telephone, fax) are to be used for that purpose, but in case that is not possible, in other written forms.

Confidentiality of Data

Article 28

(1) The data provided on the basis of this Law shall be confidential and may be used only for the detection and prevention of money laundering and financing terrorism.

(2) Submission of the data referred to in paragraph 1 of this Article to the Office, the supervisory authorities and the law enforcement authorities shall not be considered as disclosing a business secret.

…

(5) The employees in the entities and persons managing with entities who have the responsibility to undertake measures and actions for the purpose of detecting and preventing money laundering, pursuant to this Law, cannot use personal data from the clients' files for any other purpose except for performing actions of detection and prevention of money laundering and financing terrorism.

Article 33

(1) The data and reports which are received, analysed and processed by the Office are confidential and the officers in the Office shall not be allowed to use them for any other purposes, except for those determined by this Law.

(2) The Office shall keep all data or reports related to certain transactions, i.e. client, for at least 10 years from their receipt, and following the expiry of this period it may destroy them.

The aim of these provisions is to ensure confidentially of the data processed. The confidentially principles and rules should be applied and observed by both - employees within the entities and employees at the Office. Confidentiality means that the collected and processed data may be used only for detection and prevention of money laundering and financing terrorism. Any other use of the data is clearly prohibited. The Office is also obliged to keep the data for 10 years, but unlike the entities, this provision states that once this period expire the data may be destroyed. It would be much better if the words "*may destroy*" are replaced with *"must destroy"* so that is in line with the personal data processing rules.

Access and Exchange of Information

Article 34

(1) For the purpose of performing its competences, the Office can request data and documentation from all state bodies, financial institutions or other legal or natural persons.

…

International Cooperation

Article 44

(1) The Office may conclude cooperation agreements with authorised bodies from third countries, as well as with international organisations included in fight against money laundering and financing terrorism.

(2) The Office may, within the international cooperation, request data and submit the data received pursuant to this Law to the authorised bodies and organisations of third countries, spontaneously or upon their request and under condition of reciprocity, as well as to international organisations dealing in fight against money laundering and financing terrorism.

(3) The request for exchange of data from the bodies and organisations referred to in paragraph 2 of this Article should be clarified with the appropriate known facts indicating money laundering and financing terrorism and the purpose for which the requested data and information will be used.

(4) The Office shall be bound to provide all appropriate data and information upon the received request referred to in paragraph 3 of this Law in accordance with the competences set out in this Law.

(5) The Office may refuse the request for exchange of data referred to in paragraph 2 of this Article if it is contrary to this Law or if it impedes the conduct of the investigation of another competent state authority or the criminal procedure against the person on which data is requested. The Office shall be bound to elaborate the reasons for refusing the request.

(6) The Office shall be bound to use the data and information provided by the authorised bodies from third countries for the purposes laid down with this Law and under the conditions set out by the body that provided them.

(7) The Office may exchange data and information provided by authorised bodies from third countries with the bodies competent to conduct investigations, after obtaining their prior consent.

(8) The data and information provided on the basis of this Article are confidential according to the Law.

(9) The Office may request information from the authorised bodies from third countries on the manner of using the data it provided pursuant to this Article.

These two articles regulate the exchange of data between the Office and other domestic or international institutions and entities. Exchange of data is two-way communication, which means that the Office may request data from others, but it also may provide data. In this process, the Office is restricted. In the case of domestic entities, the Office may request data that is relevant to perform

its tasks. In the case of international organizations, data may be requested if there are appropriate known facts indicating money laundering and financing terrorism and if the purpose for which the requested data and information will be used is stated. Furthermore, purposes for which the data can be used by the Office are restricted – only for purposes laid down in the Law and under the conditions set out by the body that provided the data. This seems to be a good approach, because it restricts to some level the processing of data.

b) RULEBOOK ON CONTENT AND FORM OF THE DATA THAT ENTITIES SUBMIT TO THE OFFICE AND MANNER OF THEIR SUBMISSION

There are numerous bylaws adopted on the basis of this Law, but the most relevant one from the aspect of personal data protection is the Rulebook on content and form of the data that entities submit to the Office and manner of their submission. It was adopted in 2010 by the Minister of Finance. It actually further elaborates articles 29 and 31 of the Law. Provisions of this Rulebook apply to the following entities: public notaries, banks, banks, insurance companies and legal and natural persons whose business activity is buying and selling of vehicles. Each entity is obliged to use the electronic system of the Office to submit specific data. Personal data that needs to be submitted is more or less the same for all entities. It is the usual data required to identify the client: name, address and Personal Identification Number. In addition, data on the transaction is also required to be filled-in and submitted, which also is considered as personal.

The Rulebook is poor in terms of technical rules related to the use of the electronic system of the Office. As personal data is being processed through electronic communications means, than high level of technical and organizational measures must be established and implemented by the Office as administrator of the system. This Rulebook does not contain such measures, but it also fails to make a reference the possible internal acts of the Office where such measures must be introduced.

III. SUMMARY OF MAIN FINDINGS AND RECOMMENDATIONS

- In general, there is a **high level of compliance** of the entire banking sector legislation with the EU sector specific and national personal data processing rules and principles. Very small number of amendments to the laws and bylaws is necessary to be adopted in order to: a) achieve complete compliance and b) bolster the protection of the right to privacy and personal data of the data subjects (clients).
- Throughout the entire text of the Law on the National Bank, as well is in some other laws and bylaws that were analyzed, the words **"confidential data" and "confidentiality"** are used. In some cases, references to the application of the **rules on classified information** are mentioned. Many laws in other sectors have also taken this approach. Making reference to the confidentiality rules is completely wrong approach, having in mind that laws in this sector mostly regulate relations between legal entities (G2B or B2B). But it is wrongly to refer to the classified information rules, because classified information is produced only by government in case of national security or public safety. However, it is not excluded that in the process of exchange of confidential information, there might be personal data processed as well. To conclude, it would be good, but not so necessary, if there as an additional provision or reference in these laws to the adequate application of personal data processing rules.
- **The manner of regulating the personal data processing relating to the NBRM Credit Registry is good but not the best**. It is an obligation set in a law, though bit vague and not complete. Data controller/processor and data users, as well as the purpose for which the data may be used, are defined, while the details relating to the type and manner of collecting the data are to be regulated in a bylaw. Data should be treated as confidential and not as classified information. It may be reinforced by adding provision that in drafting the bylaw, the personal data protection principles and rules must be followed. Eventually, basic rules on data categories which are processed, purpose and period of processing should be given in the law.
- Article 10 of the NBRM's Decision on the contents and the manner of functioning of the Credit Registry specifies and limits the **type of data that may be provided to the Credit Registry users**. Although there is legal basis in 39 to regulate in the bylaw the type of data to be processed, yet it is a matter that should be prescribed in the law. Moreover, rights of data subject in relation to its personal data must be always prescribed in a law.

- The Law on NBRM stipulates that **NBRM will determine the type of data that it will collect from the banks**. Mostly, it will be statistical data or data of business nature. However, in some cases it might be a personal data, like in the case of the Credit Registry. Therefore, categories of data to be exchanged should be clearly stipulated by law.
- Provisions in the Law on Credit Bureau referring to the report that the credit bureau issues should be based on clear distinction between a **positive and a negative credit history register**. While positive credit history register is based on data subject consent, the negative is not, which means that the data can be provided to the party that requested it without having consent of the data subjects. This is justified because it is even in the public interest to prevent possible abuses.
- Article 19 of the Law on Credit Bureau requires that **collected data must be kept for 5 years** from the date the data subject has paid its dues or closed the account. It seems that this is a long period of time, especially taking into consideration that the obligations have been paid and there is no justifiable reason to continue keeping the data.
- It is questionable whether is the right solution put in the Law on Credit Bureau to **transfer the entire data and documents to the State Archive Office once the credit bureau ceases to operate, who should keep them for 5 years**. Data that credit bureau collects is not of archive nature and the credit bureau itself is a private entity, not a public institution. Moreover, the Archive keeps the archive documents permanently. If there is a need to transfer the data, than it should be to another state entity (e.g. NBRM), though it seems that the best solution would be to completely destroy the data.
- The only issue that might be reconsidered and modified by Macedonian Credit Bureau is related to the **manner of keeping the dossier for each data subject**. Namely, for the data subject who is a natural person his/her Personal Identification Number shall be used to identify him/her in the system and to keep the dossier. Use of this special category of data should be restricted as much as possible. It is reasonable to collect PIN, because it uniquely identifies the data subject, but there should be another method used (random numbers or characters) to identify and categorize the data subject in the MCB system. Furthermore, processing and use of PIN cannot be set in a bylaw.
- Law on Protection of Consumers in Consumer's Loans leaves to the creditor to decide what **type of information to request from the potential consumer**. It's quite understandable that assessing creditworthiness of a person will certainly require collecting of bit more personal information than other types of assessments. Question is whether wording used "sufficient information" leaves freedom to the creditor to collect personal data from the consumer, which might not be

relevant or that might be too excessive for the purposes. Therefore, this provision might be modified to avoid broad interpretations.

- The list of elements of the consumer's loans contracts ends up with "Other contractual information, if applicable". This type of phrase always gives freedom to the party that writes the contract, in this case the creditor, to add various types of information. It would be better, as proposed for other laws, to modify this phrase so that it reads ***"other contractual information, except for personal data that is not appropriate, not relevant and to excessive for the purpose of concluding the contract"***.

- The Law on Payment Operations prescribes **obligations and time periods for keeping certain documents of the accountholder and the data in the registry**. It is questionable if it is really necessary to keep payment instruments and documents which contain personal data for 5 years or this period can be shortened (are there requirements in other laws that entail to keep these records for proving purposes). Same goes for the requirement to permanently keep the data from the Single Registry of Accountholders.

- Article 15 of the Law on Payment Operations establishes the **Single Registry of Accountholders**, while article 16 prescribes that data from this registry may be used under the terms stipulated by this and other law. Basically the same data required for opening of an account, is also entered into the Single Registry. This seems appropriate and necessary in order to identify the person in the Registry and for seamless carrying out of transactions that involve different payment operations carriers. However, it should be further assessed if it is possible to have a centralized register of accounts, not of accountholders. In such case, only the account number and a bank which administers this account will be entered in the Registry.

- Decision on the manner and form of opening and closing of transaction accounts provides possibility to payment operations carrier to determine in its internal rules that other documents may be required from the accountholder and that copy of the identification document should be stored. It is understandable that the accountholder must be identified, because payment operations carrier and the accountholder conclude contract with rights and obligations. But, **requirements to store the documents that prove the identity of the contracting party, as well as to determine other documents and data to be provided by the accountholder are problematic**. The latter requirement opens possibilities for processing and storing of other documents and personal data. Therefore, it is better to clearly specify in this Decision all the documents and personal data that may be required and eliminate possibilities for the banks to determine additional personal data and to take copies of identification documents.

- Article 10 of the same Decision requires a **contract to be concluded between the payment operations carrier and the accountholder** and it sets the mandatory elements of the contract. Since the content of the contract is not limited, the payment operations carriers may add in the contracts additional data, including personal data, which it seems to be the case in the practice. It would be good to add provision in this Decision that *"personal data other the one stipulated in this Decision cannot be required and contained in the contracts*" or that "*contract shall contain only personal data that is appropriate, relevant and not excessive in relation to the purposes for which they are collected and processed."*

- The only unnecessary **data required to be entered in the registration form of non-resident investment in the country and in the registration form of resident investment abroad** is the Personal Identification Number of the authorized person to submit the application in behalf of the non-resident or the resident. It is sufficient to enter the names and contact info in these forms.

- **Measures and actions for detection and prevention of money laundering and financing terrorism** provided in the Law on Money Laundering Prevention and Other Criminal Proceeds and Financing Terrorism to great extent restrict the privacy. However, it is a global issue that the country had to follow by adopting this law and taking concrete actions to prevent or fight against these crimes. Apparently, these measures must be present and applied, regardless of the fact that they interfere into citizen's private life.

- This Law requires ID cards or passports to be used for identification purposes. All the data in the identification documents should be checked by the entities (employees) and in addition **copy of the identification documents to be kept by the entities**. It is questionable if the requirement to keep a copy of the identification document serves any purpose, because on one hand it is not a 100% certain evidence and on the other hand it might be more easily abused.

- The Office for Prevention of Money Laundering and Financing Terrorism and the entities are **obliged to keep the processed data for at least 10 years**. There is possibility for the Office given in the Law to destroy the data once this period is expired, while no such provision for the entities. It would be much better if the possibility ("*may destroy*") is replaced with obligation (*"must destroy")* and if it refers to both, the Office and the entities.

- Rulebook on content and form of the data that entities submit to the Office for Prevention of Money Laundering and financing Terrorism and manner of their submission is poor in terms of technical rules related to the use of the electronic system of the Office. As personal data is being processed through electronic communications means, than **high level of technical and organizational measures must be established and implemented by the Office as administrator**

of the system. This Rulebook does not contain such measures, but it also fails to make a reference the possible internal acts of the Office where such measures must be introduced.