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
10, Samuilova 10,1000 Skopje
Tel: (+389) 2 3230 635
Email: ipa_dzlp@dzlp.mk

Document 2.1.4-11

GUIDELINE FOR PROCESSING OF PERSONAL DATA IN THE BANKING SECTOR

Component 2

Activity 2.1.4-11

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

Table of Contents

Project office:
Directorate for Personal Data Protection
10, Samuilova 10,1000 Skopje
Tel: (+389) 2 3230 635
Email: ipa_dzlp@dzlp.mk

Support to the Directorate for Personal Data Protection
This project is funded by the European Union

I. INTRODUCTION

What is the purpose of this Guideline?

The purpose of this Guideline is to summarize the basic personal data processing principles and rules in a user-friendly manner and to provide instructions and advices for the citizens in order to improve the exercising of their personal data protection's right. The information contained in this Guideline will help the target group to better understand and exercise their data protection right in the banking sector.

Who are the addressees of this Guideline?

The Guideline is primarily designed to be a used by the citizens who as clients use the banking and other financial institutions services. The Guideline aims to educate the clients to recognize whether their personal data is handled lawfully. In addition, banks and other financial institutions (hereinafter: banks) who process personal data of their clients may also find this Guidelines useful.

How is the Guideline structured?

The Guideline is written in a way to include the most relevant legal provisions and the frequent issues that citizens face with when their personal data is processed in the banking sector. The first part of the Guideline presents and explains the most relevant personal data terms and principles, which apply "universally". The main part is dedicated to the legal obligations for those who process data in the banking sector and the corresponding rights of the clients. At the end of this Guideline, useful information on exercising clients' rights is given, including a template used for that purpose.

II. KEY NOTES ON PERSONAL DATA PROTECTION

Why is protection of personal data important?

Nowadays, citizens' right to privacy and personal data protection is rightly seen as one of the most significant human rights. It is recognized and valued worldwide. Therefore, this right has been set in the Constitution of the country. **Article 18 of the Constitution guarantees the security and secrecy of personal data!** In addition, it guarantees to the citizens protection from any violation of their personal integrity deriving from the registration of personal information through data processing. The protection extends to all areas of life of the citizens (private, professional, health services, public administration, etc.).

Huge number of persons is not aware yet of the importance of exercising and protecting this right! Many entities that collect and process data are not aware of the measures they need to take in order to protect the personal data. Sometimes, they collect personal data without legal basis or without clearly and freely given consent of the citizens. Moreover, citizens provide their personal data and agree to be publicly disclosed, although in many cases they are not bound to do so or not aware of the consequences of doing so.

Banking sector is an area where various types of personal data are processed! Most citizens are clients of banks, thus becoming personal data subject. There are more than 30 entities operating in this sector (banks, savings houses, other financial companies, etc.) that collect and process personal data. In order to open a bank account and become client of a bank, a person needs to identify himself/herself and provide personal data to the banks. When a client makes transaction exceeding certain value the bank submits data on the client and the transaction to responsible state institutions. As of all these reasons, rules pertaining to personal data processing must be well known to all, obligations must be followed by the banks and rights exercised by the clients.

What is the meaning of the most important personal data terms?

In order for the readers to get familiar with the personal data processing rules in banking sector and their rights in that respect, they need to understand the meaning of the commonly used terms. Each legal definition is followed by an example.

"Personal data" is any information pertaining to an identified or identifiable natural person, the identifiable entity being an entity whose identity can be determined directly or indirectly, especially as according to the personal identification number of the citizen or on the basis of one

or more characteristics, specific for his/her physical, mental, economic, cultural or social identity. ***In the banking sector, most frequent type of personal data collected from the clients and further processed by banks are: name, address, PIN, occupation, financial transactions, etc.***

"Special categories of personal data" are personal data revealing the racial or ethnic origin, the political views, religious or other beliefs, membership in a trade union and data relating to the health condition of the people, including genetic data, biometric data or data referring to the sexual life; therefore are subject to special restrictions on their processing. ***In the banking sector, these types of personal data of the clients are not or should not be processed.***

"Personal Data Subject" is any natural person (citizen) to whom the processed data refer. ***In the banking sector, personal data subjects are the bank clients.***

"Consent of the personal data subject" is freely and explicitly given statement of will of the citizen whereby s/he agrees to the processing of his/her personal data for previously determined purposes. ***In the banking sector, templates of contracts and requests usually contain provision which gives a choice to the client to agree on personal data processing, unless the processing of personal data is obligation stipulated in the law.***

"Controller of the Personal Data Collection" is any natural person or legal entity, a state administration body or other body, who, independently or together with others, determines the purposes and the ways of personal data processing (controller). ***In the banking sector, controllers are: banks, savings houses, credit bureaus, etc.***

"Personal Data Collection Processor" is a natural person or a legal entity or a legally authorized state administration body processing the personal data on the behalf of the controller. ***In the banking sector, those who control data also process data. In addition, other parties may also process data on behalf of the banks.***

"Personal data processing" is any operation or a sum of operations performed on personal data, automatically or otherwise, such as: collection, recording, organizing, storing, adjusting, or altering, withdrawing, consulting, using, revealing through transmitting, publishing or making them otherwise available, aligning, combining, blocking, deleting or destroying. ***In the banking sector, concluding and storing contract with the client or sending the name and amount of the loan give to the client to the National Bank are deemed as personal data processing operations.***

What are the main personal data processing principles?

Personal data shall be:

- processed fairly and lawfully on the basis of a legitimate ground;
- collected for specific, clear and legally determined purposes and processed in a manner pursuant to those purposes;
- not further processed in a way incompatible with those purposes unless the citizen has given his/her further consent;
- adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
- accurate, complete and kept up to date;
- kept no longer than is necessary for the purposes for which the data were collected and for which they are further processed.

Example from the practice: Local bank in the application for issuing of credit card requests from the clients to enter/write down the following personal data: nationality, name and surname of the spouse and his/her profession, and educational degree of the client. This type of data was considered as inappropriate, irrelevant and too excessive for the purpose it has been collected, thus not complying with the basic personal data principles.

Example from the practice: Local bank has concluded contracts with two companies – one for information security services and another one for maintenance and technical support. Both companies in providing the services (maintenance of software applications) process personal data of the bank's clients. However, the contracts signed with these companies do not contain provisions that will regulate the rights and obligations between the contracting parties in relation to the personal data processing, which is clear violation of the personal data rules.

Who has the liability and responsibility towards the clients?

If the banks wishes to engage third party to process the personal data, than it must conclude a contract with the processor by which the processor agrees to comply with principles above and to act only on the instructions of the bank. If the data processing is not done in fair and lawful manner, then the responsibility towards the client remains with the data controller. For example, if a bank wants to conduct survey among its clients and for that purpose uses the services of market research company, then: a) there should be a contract where the rules and principles on personal data processing must be set as obligation for the market research company, and b) if the personal data is not treated lawfully (abused) by the market research company, then liability towards the client remains with the mobile phone operator.

When a commercial bank, based on obligation laid down in a law, transfers personal data, for instance, to the Office for Prevention of Money Laundering, then that processing operation is not considered to be as engaging a third-party; therefore the liability towards the clients for any misuse of the transferred data is within the Office for Prevention of Money Laundering.

III. BANKS OBLIGATIONS AND CLIENTS RIGHTS REGARDING PROCESSING OF PERSONAL DATA IN THE BANKING SECTOR

How is the personal data collected and what should the client be informed about?

Banks should ensure that **collecting data is done in a fair manner** and that client's right to be informed is secured. Clients should know that **when their personal data are collected, the bank must provide them information on the:**

- identity of the bank (e.g. name and seat);
- purposes of the processing;
- users or categories of users of personal data;
- intention to communicate data to third parties, including types of recipients, purpose for which the data will be disclosed and right of the clients to object to from disclosing for specific purposes (e.g. direct marketing or quality improvement of bank services);
- compulsoriness of responding to questions and possible consequences of not responding (unnecessary questions should not be asked); and
- existence of the right to access and the right to correct personal data.

Example from the practice:
Application forms of a local bank used for consumer credit and for opening of transactional account contain provisions which condition the client his/her personal data entered in the application to be used for the purposes of direct marketing.
Similarly, another local bank in its form for identification/update of data of the client, in the part that refers to direct marketing, does not provide possibility to the client to give consent on promotional campaigns from third parties, thus processing is done in unfair manner.
In both cases the bank forms and processing were not in compliance with the personal data rules.

In addition, **clients may at anytime request from the banks information**:

- whether their personal data are being processed;
- on the purposes and legal base for personal data processing and the users or categories of users to whom the personal data are being disclosed;
- on the logic of automated processing in case such processing is applied.

What does bank secret mean?

Any documents, data and information acquired through banking activities on clients (transactions made or funds deposited by the clients) are considered as bank secret, i.e. they must be protected and kept as secret. Basically, all bank employees who have access to the documents, data and information must keep them and may use them only for the purposes they were obtained for, and are not allowed to disclose them to third parties. This obligation also

refers to other persons who, by rendering services to the bank, have an access to these documents, data and information (e.g. IT services company).

Bank secrecy requirements will not be applied in the following instances:

- if the data and information disclosure is prescribed by a law or on written request of a competent court, PRO or several other state institutions strictly defined in a law, and
- if the client gave a written consent to data disclosure.

The institutions and their employees who obtained documents, data and information must also keep them, may use them only for the purpose they were obtained for, and are not allowed to disclose them to third parties.

What type of client's data banks collect and process for their own purposes?

One of the main business activities of the banks is **giving credits** to the clients. Before the credit is approved, the bank makes an assessment of the creditworthiness of the client. In order to make better and more reliable assessment, banks are allowed to request information from the client or from a relevant database. The type of personal data that may be requested for this purpose is not legally defined, but it is prescribed that is should be data ***sufficient*** to make the assessment. It is up to the banks to decide what is going to be sufficient for them. However, they must take into account the basic data processing principles such as appropriate, relevant and not excessive.

Example from the practice: Local bank in the application for issuing of credit card and consumer credit requests from the clients to provide the following personal data: educational degree, data on the immediate family members (adults, juveniles, (un)employed), marital status of the applicant (married, single or divorced), which are inappropriate, irrelevant and too excessive for the purpose they have been collected, thus not complying with the basic personal data principles.

A person, who wants to open a **transactional account** and become client of a bank, must be identified by the bank employee. Identification means that an ID card must be presented in order to determine the name 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. Banks are required to keep a copy of the ID and entitled to request another document, if necessary, in order to determine client's identity. Opening of transactional account means that contract must be concluded that will regulate the rights and responsibilities of the contracting parties; therefore it is appropriate and relevant to process these data.

Banks must submit the data collected for the purpose of opening transactional account to the **Single Registry of Accountholders** maintained by KIBS. In addition to the account number, the following data must be provided and kept in the Register: name, address, PIN and contact information of the client – accountholder. The aim of the Registry is to provide seamless transaction process that involves different banks and to ease the work of the enforcement agents.

Banks are obliged not only to collect, but also to keep:

- ***payment instruments*** and other documents underlying the recording of changes in transaction accounts at least 5 years after the end of the calendar year in which the changes have been registered,

- ***documentation*** underlying the opening and closing of transaction account for 5 years after the end of the year in which the transaction account has been closed, and

- ***data*** from the transactional account registry permanently.

What type of client's data banks collect and process to the National Bank?

Banks must submit data needed for the purposes of the **Credit Registry established and maintained by the National Bank**. The type of data processed for this purposes is mostly of personal nature, i.e. data that identifies the client (name, address and PIN) and his/her payment obligations. Clients have right to enclose evidence to the bank that their personal data in the Credit Registry are incomplete, inaccurate, or not updated. If there is a written request, the bank must supplement, modify, delete or replace the data simultaneously with accurate data, or terminate the use of incomplete, inaccurate, or not updated data, simultaneously replacing them with accurate ones. The data maintained in this Registry can be provided upon a written request to the legally determined third parties - Credit Registry users.

What type of client's data banks collect and process to the Macedonian Credit Registry?

In addition to the Credit Registry maintained by the National Bank, the law provides possibility for private companies to establish credit bureaus. Main business activity of these bureaus is processing data about clients and providing accurate reports on the financial obligations and on the regular payments of these obligations by the clients. Credit bureaus 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.

These registries are broader than the Credit Registry maintained by the National Bank, because data on all payment obligations of the citizens may be processed (e.g. debts towards utilities providers such as water supply or electricity). Personal data that may be processed by the credit bureau is data necessary to identify the data subject such as client's name, address, PIN and payment obligations.

Credit bureau in issuing the report and providing personal data to the users must follow data processing rules:

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

The most important rule is that without a **consent given by the client** the credit bureau cannot provide the report to the data user.

Processed data must be kept for 5 years from the date the client has paid its dues or closed the account.

Credit bureau has the following obligations towards the clients:

- obligation to provide to the client information on data providers and data users,

- obligation to present to the client his/her rights,

Clients have the following rights:

- right to withdraw the given consent,

- right to dispute the data contained in the register and/or report.

The obligation to provide accurate and up-to-date data and to correct the data upon a request of the client has to be followed by the data provider as well.

In 2010, the first and so far the only **Macedonian Credit Bureau (MCB)** was founded by KIBS. So, all above mentioned obligations must be followed by MCB. It should be mentioned that MCB in its Rulebook on Operations stipulates that if the data processed by MCB is wrong or there is no longer need to keep the data in the register, the data will be deleted.

What should be undertaken by the banks from technical and organizational point of view to ensure secrecy of clients' data processing?

Banks are obliged to adopt and implement appropriate technical and organizational measures to ensure the security of their networks and/or services and to protect the personal data they process from any accidental or illegal damaging. Measures are categorized at three levels: basic, medium and high. The level to be implemented depends on foreseeable risks and nature of the data being processed (e.g. if a bank provides to its users e-banking services than high level measures must be implemented).

Security measures include, among others, security of the buildings in which the personal data are stored and/or processed (including access to the building), list of authorised persons (with a mention of their liability) to access the data, appropriate authentication mechanisms (e.g. passwords control), security in the transfer of data between the data controller and the data processor, encryption of the media used to store or transfer data, etc.

Example from the practice: Local bank did not protect the premises where the digital video recorders are located from the risks of potential fire, explosions and smoke, because they kept in the same premises other materials and things that are easily combustible.

Another local bank did not configure its information system in a manner that after 3 unsuccessful attempts to login the person will be automatically rejected.

In both cases, the banks infringed the personal data processing rules.

IV. MEASURES AND ACTIONS FOR PREVENTION OF MONEY LAUNDERING AND FINANCING TERRORISM *vis-a-vis* PERSONAL DATA PROTECTION

Why are measures and actions introduced?

The aim behind prescribing measures and actions to be undertaken by various entities is to detect and/or prevent money laundering and other criminal proceeds and financing terrorism. These measures and actions to great extent restrict the citizen's privacy. However, it is a global phenomenon and the country had to follow and accept obligations deriving from international organizations and agreements, regardless of the fact that they interfere into citizen's private life. Still, there are some limits set for the entities that must implement the provisions from the Law on Prevention of Money Laundering and Other Criminal Proceeds and Financing Terrorism, thus protecting the data processed.

What are the measures and actions that banks must undertake?

For these purposes, the banks must take the following measures and actions:

- client due diligence;

- monitoring of certain transactions;

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

- introduction and application of programmes.

Banks must apply client due diligence procedures in the following cases:

- when establishing a business relationship – e.g. opening of transactional account or of a client;

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

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

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

Client's due diligence procedure includes:

- identification of the client and verification of his/her identity;

- identification of the authoriser and verification of his/her identity and identification of the beneficial owner and verification of his/her identity;

- obtaining information on the purpose and intention of the business relationship; and

- conducting ongoing monitoring on the business relationship.

When do the banks submit the processed data to the Office?

Banks are bound to submit the data collected, the information and the documents to the Office in the following cases:

- 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,

- in case of cash transaction in the amount of EUR 15,000 in denar counter value or more, and

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

This is general obligation that refers not only to the banks, but also to other types of entities. They are all obliged to collect data, but they are not obliged to further process each data to the Office. In addition to this general obligation, banks are also obliged to submit data in case a credit in amount exceeding EUR 15.000 is given to a client.

For how long the banks and the Office keep the personal data?

Banks are obliged to keep the records relating to the transactions for a period of 10 years.

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

Should the confidentiality principle be followed?

Data collected for the purpose indicated above is deemed as confidential and may be used only for the detection and prevention of money laundering and financing terrorism! This means that employees in the banks and persons who have the responsibility to undertake measures and actions for the purpose of detecting and preventing money laundering, 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.

Data and reports processed by the Office are also deemed as confidential and the officers in the Office are not allowed to use them for any other purposes, except for those determined by the

law.

If the readers would like to have more information on the prevention of money laundering and financing terrorism and work of the Office, we recommend them to visit the following web site: http://www.usppft.gov.mk/

IV. USEFUL ADVICES ON EXERCISING THE CLIENT'S RIGHTS

What rights does the client have in regards to the data changes?

Upon the request of the client or if bank determines on its own, the bank must supplement, amend, delete or prevent the use of the personal data, if they are incomplete, incorrect or not updated and if their processing is not in conformity with the law.

Who should the client turn to in order to exercise the rights?

Right to object to the processing of his/her data shall be exercised in the first instance before responsible person/officer of the bank. Each bank has appointed personal data protection officer. This person/officer must implement procedures that enable rights to be exercised in a simple, fast and efficient manner, which do not entail undue delay or cost (respond to a client request must be given within 15 days). When a responsible person concludes that exercise of rights is not justified, the client should be informed of the reasons that led to this conclusion.

How can the right to complain be exercised?

If the client is not satisfied with the responses and information given by responsible person/officer within the bank, and considers that his/her rights are violated or information provided insufficient, s/he can submit a request to the Directorate for Personal Data Protection (DPDP) for confirming violation. ***How to submit complaint for personal data protection?***

It's very easy and simple. Whenever one believes that her/his right of personal data protection is violated and has some facts or prove for the violation, s/he can submit to the Directorate for Personal Data Protection:

Request (complaint) for determining a violation of the right of personal data protection or
Initiative to the the Directorate to perform inspection over the personal data processing performed by the controller of personal data collection.

In order to facilitate these procedures, the Directorate has developed forms of Request (complaint) and the Initiative for performing inspection, which are published on the Directorate's web site (www.dzlp.mk/mk/prijavi zloupotreba).

What is the role of the Directorate for Personal Data Protection?

For the purpose of supervising the lawfulness of the undertaken activities while processing and protecting personal data, a DPDP is established as an independent state body. DPDP main task that is of interest to the clients is the resolving clients' complaints for violation of their data protection rights.

Project office:
Directorate for Personal Data Protection
10, Samuilova 10,1000 Skopje
Tel: (+389) 2 3230 635
Email: ipa_dzlp@dzlp.mk

Even if there is no request submitted, DPDP inspectors may, within the inspection supervision, among other measures order:

- blocking, deletion or annihilation of the personal data;

- completion, updating, correction, revealing or providing personal data secrecy;

- implementation of additional organizational and technical measures for securing secrecy and protection during the personal data processing; and

- prohibition for further personal data processing.

DPDP also has an awareness raising and advisory role and for that purpose provides guidance on the protection of personal data and conducts training to the interested parties, especially data controllers and processors.

To find out more about the work of DPDP and other useful information relating to personal data protection, please visit the following web site: http://dzlp.mk/mk