ČESKÁ BANKOVNÍ ASOCIACE
CZECH BANKING ASSOCIATION

RECOMMENDED INTERPRETATION OF CERTAIN PROVISIONS OF GDPR IN THE BANKING SECTOR

Praha I 15. 04. 2019

Table of Contents

This document provides a framework for the interpretation of certain provisions of Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation, hereinafter the "GDPR") in the processes of providing banking products and services which takes into account the specificities of the banking sector and its dependence on the processing of personal data in a large scale. The aim of the document is to lay down the interpretative framework of the banking sector used in the application of the GDPR with a view to ensure compliance with other financial market regulations at the same time and take into account the specifics of the banking sector in the interpretation of the individual provisions of the GDPR.

These recommended practices do not represent a binding interpretation of the relevant provisions; it is up to each bank to consider how it will interpret GDPR. However, the interpretation given below is accepted by all Members of the Czech Banking Association who will subscribe to this document. The document represents a generally conceived minimum level of protection of personal data subjects and individual Member Banks are not prevented from choosing a higher level of personal data protection in specific cases, based on their specific needs and practices.

In their business, banks are subject to extensive regulation in all areas of providing banking products and financial services. In relation to natural persons, this includes in particular implementation of the requirements of directly effective European regulations or directives transposed into the legal order of the Czech Republic, for instance, by the Act on Banks, the Consumer Credit Act, the Act on Selected Measures against Legitimisation of Proceeds of Crime and Financing of Terrorism, the Payment System Act, etc. The GDPR establishes a basic framework for the processing of personal data, which banks have to combine with their other legal and regulatory obligations.

Banks process personal data of their clients and potential clients, employees, suppliers and other persons (such as members of the Supervisory Board) in accordance with the requirement of lawful processing (Article 6 of the GDPR) on the following legal bases:

- The processing of personal data is necessary for the conclusion of a contract and its subsequent performance (Article 6 of the GDPR, paragraph 1 (b)); this includes, for instance, the processing of identification and contact details prior to the conclusion of the contract or adding data during a contractual relationship, such as change of surname, updating of contact details, etc.
- Personal data are processed for compliance with a legal obligation imposed on banks by a binding legal regulation (Article 6 of the GDPR, paragraph 1 (c); this involves, for instance, data obtained from clients of banks in connection with mandatory measures aimed against the legitimization of proceeds of crime or data, concerning credit exposure and payment behaviour when negotiating consumer credit, etc. [1];
- The processing of personal data is necessary in order to protect the vital interests of clients (Article 6 of the GDPR, paragraph 1 (d);
- Banks have a legitimate interest in the processing of personal data - this legal basis is balanced by the rights of the data subject (Article 6 of the GDPR, paragraph 1 (f); this includes, for instance, sending marketing messages to bank clients, processing data for risk management purposes, etc.;
- Personal data are processed for a specific purpose based on the consent given by the data subject to the bank (Article 6 GDPR, paragraph 1 (a), while such consent is expressed in accordance with the conditions laid down in the GDPR (Articles 7 and 4 – the consent is verifiable, informed,

[1] In banking, many obligations are also based on secondary legislation, or indirectly from the interpretations or the decision-making practice of the regulator (most often the CNB).

freely given, understandable and revocable); consent is required, for example, where third party products are offered that are not related to the offer of banking products, or when the bank processes personal data by so-called profiling for marketing purposes, etc.

A) SPECIFICS OF CERTAIN LEGAL BASES FOR THE PROCESSING OF PERSONAL DATA

1. Data processing on the basis of a legitimate interest (the "proportionality test" and objections)

Proportionality test

Where the bank intends to process personal data based on the legal title of a legitimate interest, it will perform a proportionality test assessing its legitimate interest in the processing against the fundamental freedoms and rights of the data subjects thus ascertaining whether a real legitimate interest in connection with the given processing belongs to it or not. The proportionality test consists of three basic parts:

- Defining the legitimate interest;
- Establishing that the data processing in question is necessary for achieving of the legitimate interest;
- Assessing the alleged legitimate interest against the interests and fundamental rights and rights of the data subject.

Where, as a result of the proportionality test it is concluded that the interests, fundamental freedoms and rights of the data subjects override the given legitimate interest of the bank, the bank may not process the personal data in question on the basis of a legitimate interest.

Developing internal methodology describing in which cases, how and by what criteria the proportionality test should be developed, including laying down rules for its archiving and rules for possible consultations with the Data Protection Officer where appropriate, can be given as an example of good practice. It is at the discretion of the bank to decide whether to opt for a proportionality test in the form of a verbal or numerical assessment. The proportionality test should be made out in a written form so that it may serve as evidence of implementing the process described above.

Objections

The data subject has the right to object at any time, on grounds relating to his or her particular situation, to the processing of personal data on the basis of a legitimate interest (unless the objection is raised against the processing of personal data for the purposes of direct marketing on the basis of a legitimate interest, as described in more detail below). Therefore, the bank may request the data subject to describe the reasons relating to his or her particular situation, which make him/her believe that the bank has no legitimate interest in processing his or her personal data, in the objection raised by him/her. Until the moment when the data subject specifies these reasons, it is not an objection within the meaning of Article 21 (1) of the GDPR.

In the event of an objection which has been properly raised by the data subject, the bank shall no longer process the personal data (it shall restrict their processing) until it has verified that its legitimate reasons for the processing of the personal data that should be described in the proportionality test

override the interests or rights and freedoms of the given data subject. The restriction of the processing of the personal data in question relates only to the opposed purpose of the processing; thus, the bank may continue to process them for other purposes, for which it has legal grounds. Restrictions on the processing of the personal data in question also do not apply to the processing which is necessary for the establishment, exercise or defence of legal claims, in which case it is not only the legal claims of the bank, but also the claims of third parties that may be involved. For more details on the processing of personal data, please see also Chapter B) Article 1, paragraph 1.1 of this document.

Special rules shall be applied to the application of an objection to the processing of personal data for the purposes of direct marketing based on a legitimate interest - the data subject does not have to substantiate the objection and the objection is effective without any further action.

The right to object to the processing of personal data on the basis of a legitimate interest (for the purposes of direct marketing and for other purposes) should be explicitly brought to the attention of the data subject and should be presented clearly and separately from any other information at the time of first communication with the data subject at the latest. This obligation shall be deemed fulfilled also where information on the right to object to the processing of personal data is disclosed in the text by which the bank fulfils its obligation to provide information to data subjects in accordance with Article 13 or Article 14 of the GDPR provided that the text is clearly separated from other information, for instance contractual information.

2. Consent to the processing of personal data and its conditions

2.1 GDPR Consent

a) Basic rules for obtaining consents to the processing of personal data

- The provision of a banking service shall not be conditional upon the giving of consent to the processing of personal data by the data subject.
- Data subjects may be positively motivated to give consent (for instance, by providing a reasonable discount).
- The consent must be easily revocable and the data subject must not be penalized for withdrawing the consent.
- Data subjects may not be required to express disagreement but only to express consent, since the GDPR knows only consent expressed by active conduct, (i.e. the consent must be based on the *opt-in* principle).
- Consent need not be given on a separate form and may be part of another document but it must be distinguishable from other text and the data subject must be able to express his or her will to give consent (for instance, by ticking a box).

b) Minimum requirements for the content of consent to the processing of personal data

- The purpose of the processing (consent may contain several different/incompatible purposes; however, the data subject has to be enabled to freely express himself/herself with respect to each individual purpose, i.e. the individual purposes must be separable)
- The scope of the processed personal data
- Identification of the controller:

- All controllers to whom the consent is given have to be identified (but it is not necessary to give consent to each controller separately on a form)
- Each controller should be identified by the name (business firm) and the identification number, where appropriate and adequate to the particular type of communication
- A foreign controller must be identified by the name (business firm), the legal form and registered office

- Information about the data subject's right to withdraw consent, or the right to lodge objection (comment, manual review, the right to challenge the decision) to automated decision-making, if it is performed on the basis of consent.

The period for which consent is given to the processing of personal data is not a mandatory requirement regarding the content. Information relating to the data subject's rights does not have to be contained in the consent form. The text of consent may contain a reference to another document (information memorandum) with further information on the processing of personal data required by the GDPR.

2.2 Consent pursuant to other legislation and making copies of identity cards

a) Making copies of documents when identifying persons

In their activities, banks must use procedures to prevent the use of the financial system for money laundering or terrorist financing. To that end, they are governed by the national legislation which implements Directive of the European Parliament and of the Council (EU) of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, which has been implemented in Act No. 253/2008 Coll., on Certain Measures Against Money Laundering and Terrorist Financing (hereinafter referred to as the "AML Act").

The key principle of this activity is to identify all persons connected with the banking product or service. For this purpose, banks ("obliged persons") carry out identification of persons by being allowed, inter alia, to make copies or extracts from the submitted documents (in the case of an identity card with the consent of the client) and to process the information thus collected if required by the AML Act or if it is necessary to achieve its purpose.

In addition to identification documents, banks are also obliged to store copies of documents and information obtained in the context of client checks in accordance with Section 9 of the AML Act. The client check is carried out, inter alia, at the establishment and during the course of the business relationship, when effecting a transaction above a certain financial limit, or where there is a suspicion of money laundering or terrorist financing, when establishing a business relationship with a politically exposed person or a client established in a risk country.

If the bank, in its activities resulting from the AML legislation, makes copies of documents submitted during the identification or a client check, it is required by law to store them for a period of 10 years from the execution of the transaction or from the termination of the business relationship with the client. The client does not give consent to storing these documents and his/her possible disagreement does not have any effect on their storage. The time limit shall run from the first day of the calendar year following the year in which the last business transaction was performed known to the obliged person.

b) Consent with processing the personal identification number

The processing of the personal identification number is governed by Act No. 133/2000 Coll., on register of population and birth numbers, and on amendments of certain acts (Register of Population Act), as amended. This act taxatively defines the cases when the personal identification number can be used. One of these cases is a situation where this is stipulated by a special law. For banks, such a law is the Act on Banks, which states that "*For the purposes of banking transactions, banks and foreign bank branches shall collect and process the data on entities, including the birth number, where allocated (excluding sensitive data on natural persons) necessary to allow the banking transaction to be executed without the bank incurring undue legal and material risks".* At the same time, the AML Act, too, sets out the obligation to obtain the identification data of the client in Section 5, which includes, inter alia, the personal identification number, if allocated, as one of the basic identification data.

For the above reason, banks do not require from their clients or from other persons whose data they process in bank transactions, consent to process the personal identification number**.**

B) INTERNAL OBLIGATIONS OF A BANK

1. Records of processing activities

The bank, both as the data controller and the data processor, is obliged to maintain records of processing activities. The basic content of the records of processing activities is provided for in Article 30 of the GDPR. The bank differentiates between records of processing activities in the capacity of the controller and records of the processing activities which it performs as the processor.

In practice, there may be situations where the bank is generally in the position of the controller of personal data but it also performs certain processing for another controller, and in relation to these processing activities and personal data, it is then in the position of the processor at the same time. In this case, one record of processing activities can be developed if the cumulation of activities in one record of processing activities seems appropriate to the bank as the controller.

Forms of records of processing activities

The bank shall individually lay down a single (framework) structure of records of processing activities. The structure of the records selected by the bank should be clear and understandable. In terms of content, records shall at least contain information specified in Article 30 (1) of the GDPR where the bank is the data controller, or in Article 30 (2) of the GDPR, if the bank is the data processor. Records of processing activities may also contain information that the GDPR does not require, for instance whether DPIA was prepared for the processing activity or in which systems personal data are processed. The bank is not obliged to include complete documentation relating to the processing activity in the records; it may refer to the documentation (for example by referring to an internal policy on technical and organizational measures). Likewise, records of processing activities may contain references to the relevant policies.

Preparation and reviews of records of processing activities

Records of processing activities are drawn up by the bank prior to starting the processing activity. If the process of processing activities which is already under way is changed, the bank updates the processing activity record at the same time as when the change in the processing activity is introduced at the latest. The bank reviews records of processing activities at regular intervals.

A development of an internal methodology that describes the rules for the preparation of records of processing activities, their content, the responsibility of the bank staff for the preparation of the record of processing activities and for keeping it up-to-date, and the rules for the life cycle of records of processing activities, can be given as an example of good practice.

Granularity of records of processing activities

Depending on the nature of the particular processing, the bank may proceed to differentiating the records of processing activities. The bank may internally determine what criteria it will use to group processing activities into records of processing activities. An example of good practice can be a breakdown of records of processing activities in accordance with the purpose of the processing, or according to its processes (for instance in accordance with certain agendas), products, or according to its technical conditions (for instance, taking into regard its systems). If the bank selects a breakdown of the records of processing activities in accordance with a different criterion than the purpose of the processing, one processing activity may include more than one processing purposes.

2. Data protection impact assessment

The assessment of the impact of personal data processing on the data subjects is also known as the DPIA, the English acronym for the d*ata protection impact assessment* and is a means for managing the risks associated with the processes of personal data processing newly introduced by the bank.

The bank should consider whether or not it should carry out the data protection impact assessment in connection with any new processing of personal data or modification of the existing processing.

The DPIA has to be always carried out where:

a) A type of processing, in particular processing using new technologies, is likely to result in a high risk to the rights and freedoms of natural persons, taking into account the nature, scope, context and purposes of the processing; or
b) The intended processing is on the list of the types of processing operations published by the supervisory authority which are subject to the requirement for a data protection impact assessment.

Article 35 (3) of the GDPR defines the basic cases in which the processing of personal data is likely to result in a high risk to the rights and freedoms of natural persons and the DPIA is therefore required. More specific criteria that have to be taken into account in assessing whether or not the DPIA is required were defined in the guidelines of the European Data Protection Board[2]. As an example of good practice, the DPIA should always be carried out whenever at least two of these conditions are met, unless the bank assesses that the particular processing does not, however, represent a high risk-such a decision is always carefully justified and documented.

[2] Guidelines on Data Protection Impact Assessment and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP 248 rev.01, in the updated version from 4 October 2018, are avilable at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.

On the other hand, there are situations where the DPIA is not necessary, namely if:

a) The nature, scope, context and purposes of the processing are very similar to those for which the DPIA has already been carried out by the bank;
b) The processing operation has been reviewed by the Office for Personal Data Protection prior to May 25, 2018, under specific conditions which have not changed;
c) The processing has a legal basis in Union law or in the law of the Member State if that law governs the specific processing operation and where a data protection impact assessment has already been carried out in the context of the adoption of the above-said legal basis unless a Member State declares that it deems it to be necessary to carry out such an assessment prior to processing activities;
d) The specific processing is included in the list of the types of processing operations for which the data protection impact assessment is not required, provided that such a list has been published by the supervisory authority.

The Office for Personal Data Protection issued its list of such types of processing operations[3], which, although it is not binding until the moment of its approval by the European Data Protection Board, may be taken into account by the bank when assessing the need to carry out the DPIA.

Where it is assessed that the DPIA is required, the bank must undertake at least the following as part of the DPIA:

a) A systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
b) An assessment of the necessity and proportionality of the processing operations in relation to their purposes;
c) An assessment of the risks to the rights and freedoms of data subjects; and
d) A description of the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR.

Within the banking sector, the obligation to prepare DPIA typically touches on matters such as:

- The introduction of new processing involving biometric data (for instance face authentication – “face ID” or voice authentication);
- Introduction of a new sales channel of the bank (such as a new on-line platform);
- Introduction of a new automated scoring process for clients;
- Introduction of an entirely new product.

The bank shall, where appropriate, engage the relevant third parties, possibly including the data subjects, or their representatives, in the process of the DPIA described above in the form of consultations. Where the bank identifies risks to the rights and freedoms of natural persons in the process of the DPIA, that cannot be mitigated by appropriate measures in terms of available technology and costs of implementation, a consultation of the processing with the Office for Personal Data Protection has to take place.

Banks are not required to publish the DPIA results. The DPIA is not a one-time process, and the bank therefore periodically reviews compliance with the DPIA's findings within the established processes and verifies whether there has been a change in input parameters or risks that would justify a reassessment of the current process and possibly the launch of a new DPIA process.

[3] Draft list of the personal data processing operations which are not subject to the data protection impact assessment is available at: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=30738.

Development of an internal methodology that describes the relation of the DPIA to project (change) management, the responsibilities of individual bank employees, including their involvement in the DPIA process and the criteria for assessing whether the DPIA is required or not, development of the DPIA itself and of its life cycle, can be described as an example of good practice. It is at the discretion of the bank to decide whether to opt for the DPIA in the form of verbal or numerical rating.

3. Data retention period

(For the purposes of this document, the retention period starts to run at the moment when the contract between the bank and the client is terminated.)*

Banks as controllers of personal data have numerous obligations that they have to perform when processing personal data, including the obligation to store personal data about clients and banking operations for the purposes of fulfilling the obligations laid down by the sectoral regulation. In accordance with the "storage limitation" principle, such data should be kept in a form which permits the identification of data subjects for no longer than is necessary for the purposes for which they are processed. From the point of view of the GDPR, it is possible to find support for lawful processing in the performance of banking activities in the case of personal data storage especially within the limits of the following legal grounds:

I. Processing required for **compliance with a legal obligation** (imposed by sectoral regulation, including specific time periods for such storage) applicable to banks, in particular by:

a) Act No. 21/1992, Coll., the Act on Banks (hereinafter referred to as the "ZoB"), which provides, in particular, for the processing of personal data necessary to execute the transaction and assess the risk;
b) AML Act, which obliges banks to process personal data, especially for the purposes of identification and subsequent due diligence of the client;
c) Act No. 256/2004 Coll., on Business Activities on the Capital Market (hereinafter referred to as "ZPKT") relating in particular to records of communications and documents relating to the investment service provided;
d) Act No. 499/2004 Coll., the Act on Archives and Records Service, relating to the retention of personal data for archival purposes.

II. Processing required for the **purposes of the legitimate interests** of the bank, in particular with respect to

a) The exercise of rights in civil proceedings

Act No. 89/2012 Coll., the Civil Code (hereinafter referred to as "OZ"), which lays down a limitation period of 15 years for intentionally caused damage or injuries and deliberately acquired unjust enrichment. For this reason, the bank should have a legitimate interest in archiving client data for a period of 15 years (until the potential claims of the client are time-barred).

b) The exercise of rights in criminal proceedings and
c) The exercise of rights in administrative proceedings

The limitation periods for misdemeanours and criminal acts, which the bank, or persons acting on its behalf respectively, could potentially commit, will also have an influence on the time period during which the bank has to keep the data in order to protect its rights. For the purposes of proving that no misdemeanour or criminal act have been committed, the bank should store the data on the

transactions executed, in justified cases, for up to 15 years from the end of the transaction, unless further retention is necessary in the particular case. The limitation period for misdemeanours arising from the ZoB, AML and ZPKT is 3 years (Act No. 250/2016 Coll., on Liability for Misdemeanours and Related Proceedings), the limitation period of criminal acts is based on Act No. 40/2009 Coll., the Criminal Code (hereinafter referred to as "TZ"). Criminal acts which could be committed by the Bank are subject to a 15-year limitation period (for instance, embezzlement, fraud, insider trading, etc.)

Given the fact that the limitation period may be suspended in all the above cases, it is in the interest of the bank to store personal data for a further 3 years after the expiration of the 15-year period which commences upon the execution of the transaction.

4. Conditions governing the retention of personal data

Banks have an obligation to ensure that information relating to the purpose of processing, categories of personal data, categories of data subjects, categories of recipients and to the **storage period** are communicated to the data subjects (clients) prior to the **start of processing**, in **fulfilment of information obligations**.

In order to maintain the principle of proportionality, it is necessary to assess the processing (storage) of personal data individually and **not apply time limits in a blanket manner** so that **personal data are not** stored for longer than is necessary for the purpose of processing. In order to ensure that personal data are not stored longer than necessary, banks should also periodically **review the retention periods for personal data,** including supporting documentation.

Additionally, **appropriate measures** have to be implemented to provide for the **rectification or erasure of personal data,** which are the subject of the processing in order to **respect the rights of the data subjects**, in particular the right to have his or her personal data erased and not further processed where the legal ground for their processing no longer exists.

In addition, **technical and organisational measures** shall be established to prevent their unauthorised processing, in particular the adoption of such measures that lead to **ensuring** their **security, confidentiality and integrity**. Where banks use a processor for some of their activities, they are also obliged to ensure that **the processor returns or erases the personal data** after the processing has ended, if the personal data are not required to be stored under Union law or the Member State law applicable to the processor.

As for the **form of the retention of personal data**, personal data should be further processed only if the purpose of processing cannot be reasonably achieved by other means. In such case, it is necessary to keep in mind the rights of the clients **to protection from unauthorized interference in private and personal life** and to **erase personal data or possibly to pseudonymise them** as soon as possible, i.e. not process them in a form enabling the identification of the data subject.

In each situation, banks have an obligation to assess the specifics of the processing, including individual setting of the corresponding retention period, which they will be able to justify. Banks have also a duty to take such technical and organizational measures as to ensure adequate protection of the retained personal data.

C) CUSTOMER RELATIONSHIP

1. Ensuring the rights of the clients

1.1 Right of restriction of processing

Pursuant to Article 18 of the GDPR, the controller is obliged to restrict the processing of personal data of data subjects in several exhaustively defined cases. This is a situation where:

- The accuracy of the personal data is contested by the data subject[4]
- The processing is unlawful or no longer needed to achieve the purpose and the data subject requests them to be maintained instead of the erasure[5]
- The data subject raised an objection to the processing of personal data based on the legitimate interest of the controller or of another person[6]

Restriction of processing, as defined in the provisions of Article 4 (3) of the GDPR, means flagging the data in question in a way restricting their processing in the future. According to the relevant list, methods by which to restrict the processing of personal data could include, inter alia, temporarily moving the selected data to another processing system, making the selected personal data unavailable to users, or temporarily removing the data from publicly available websites. [7]

The technical solution of the restriction of processing will generally always depend on the system and the means in which, respectively, through which, the data are processed, whether automatically or manually. The restriction may, taking regard of the scope of processing, the complexity of technical means, and the obligation of the bank to provide other services to the client who has raised the objection, also be implemented by adding a specific flag to the data. Therefore, this does not necessarily mean only blocking or hiding the data.

For the bank, restriction of processing represents, or may represent a significant interference and is associated with other costs, in particular with regard to the restrictions on processing of data in accordance with Article 18 (2) of the GDPR (and thus, for example, with the need to obtain the consent for further processing required for the fulfilment of the contract, processing of an application for a new product or modification of the existing one, etc.) and to its obligation to inform data recipients of the restricted processing (other entities within the group, processors, operators of banking and non-banking registers, etc.). There is also a risk of misuse of this right where the data subject will knowingly lodge unjustified or unreasonable objections in order to restrict the processing of his or her data for at least some time during, for example, recovery of a claim.

For the above-mentioned reasons, it is essential for the bank to request the client who lodged the complaint to restrict the processing of his/her data to provide at least a basic justification for such complaint. It is also necessary to request that the complaint meets the general requirements in accordance with the civil law, that it is, in particular, precise and understandable and that the data subject concerned is sufficiently identified.

The complaint contesting data accuracy must contain a specification of the data or category of the processed data which, according to the client's opinion, are inaccurate, and the client should at least indicate (or directly attach) evidence to support his/her claim. Only in this case will the bank proceed to restrict the processing (and also inform the data recipients) and initiate a review of the complaint.

[4] Article 18 (1) point a) of the GDPR.
[5] Article 18 (1) points b) and c) of the GDPR.
[6] Article 18 (1) point d) of the GDPR.
[7] List included in Article 67 of the GDPR.

In the event that the client seeks to restrict the processing due to inaccuracies of personal data, the bank will only restrict the processing of such personal data which are contested to be inaccurate (the client, for example, objects that his/her contact address is inaccurate and the bank does not send any communications to that address for the period of restricted processing); however, other personal data may continue to be processed without restrictions. In the cases referred to in Article 18 (1) (b) and (c) of the GDPR, the bank is obliged to comply with the data subject's request and restrict the processing only on condition that such a request is delivered to it before the erasure of personal data.

Restriction of processing may also have a direct impact on the services provided by the bank. While the client may not be aware of this, the restriction of processing may result in a conflict with the obligation to provide a service (the service as such or a service with certain parameters) in accordance with a special legal regulation. An example of best practice is a procedure where the bank first reviews the request for restricting processing at the basic level also from the perspective of the impact on the services provided, and if such a significant impact on the client is identified, it will call the client's attention to this consequence and to the possibility of expressing consent to the processing which is necessary for that service [8].

1.2 Right to erasure

The GDPR codifies a new concept, namely the right to the erasure of personal data, respectively "the right to be forgotten".

Conditions under which the controller is required to erase the person's personal data are exhaustively listed in Article 17 (1) of the GDPR. Exceptions from them, respectively situations, where the controller is not obliged to erase the data, are then laid down in Article 17 (3) of the GDPR.

Situations where the person concerned can exercise the right to erasure can be divided into several groups of cases:

- Retention or other processing of personal data of the person concerned is unlawful[9]
- A legal obligation has been imposed on the controller to erase personal data[10]
- The person concerned withdraws consent to personal data processing and the controller has no other legal grounds for their processing[11]
- Application of the opt-out principle from data processing for direct marketing[12]

No specificity is found in the activities of the bank in the first two cases. If the processing of personal data is unlawful or where an obligation has been imposed on the bank to erase the data, the bank is obliged to act in accordance with the law.

Only a very small part of the processing of personal data takes place in a banking environment on the basis of the consent of the persons concerned. As regards clients, the bank is obliged by the sectoral regulations, in particular by the ZoB, AML, Act No. 257/2016 Coll., on Consumer Credit (hereinafter referred to as "ZSÚ") or by ZPKT, to identify the client and store his/her data and the data relating to transactions with him/her even for many years after the termination of the business relationship. Regarding employees, the bank is obliged to manage personnel security as part of its prudential rules, in relation to certain groups of employees, the obligation is imposed on it by special laws (the ZSÚ, the Insurance and Reinsurance Distribution Act and in the case of certain banks, by the Act on Cyber

[8] Article 18 (2) of the GDPR.
[9] Article 17 (1) points a), c) and d) of the GDPR.
[10] Article. 17 (1) point e) of the GDPR.
[11] Article. 17 (1) points b) and f) in combination with Article 8 (1) of the GDPR.
[12] Article. 17 (1) point c) in combination with Article 21 (2) od the GDPR.

Security). Also, the obligation to process and store a number of employees' data, resulting from special laws, or to protect their or the bank's legitimate interests, is imposed on the bank as an employer.

With regard to direct marketing, it should be noted that the legal norm in question does not have immediate effect on marketing communications sent electronically, i.e. on communications sent to electronic contacts (e-mail, telephone number) because they have a separate legal regime (see Article 95 of the GDPR, which refers to the ePrivacy Directive, the part of which is transposed by Act No. 480/2004 Coll., on certain information society services). Therefore, it has effect on direct marketing in the form of offers sent physically, on telephone calls and on the processing of personal data and related profiling when preparing offers sent electronically. In the case of clients or other persons whose data the bank has an obligation to retain in accordance with the above-mentioned legal regulations and whose data are necessary for the execution of banking transactions and the fulfilment of the legal obligations of the bank, the bank cannot erase them even after disagreement with direct marketing was expressed. The exception contained in Article 17 (3) (b) of the GDPR shall be applied to this situation. Actually, in this case, it would be in particular an expression of refusal of processing for the purpose of direct marketing and a case of a possible erasure of derived data used only for marketing, typically a consumer profile, rather than erasure of data as such. [13]

The overall conclusion is that none of the cases described above are actually new regulations, because the controller had been obliged to proceed in the same way in accordance with the previous legal regulation. In practice, the complete erasure of personal data processed by the bank will usually occur only in the case of persons who are not clients or applicants for a product of the bank, or its employees, but whose data have been collected and processed by the bank for marketing purposes in particular.

In connection with the erasure of personal data, either at the request of the person concerned or in a regular process set by the bank, several procedural or technical aspects should be specified in the light of the specifics of the banking environment:

- ✓ If the bank intends to erase personal data, should it also erase records that it has processed them in the past and when it erased them?

A solution to this issue has to be based primarily on the meaning of the right to erasure, which is usually an irreversible destruction of other than identification data (direct identifiers), in particular the data on purely personal, economic, social or cultural identity. On the other hand, mere storage of the identification data of the subject, not their active use, together with information about which categories of personal data, and possibly in which period and for what purpose have been processed by the controller and information on the realisation of the erasure, particularly in the form of a log, as well as the related communication with the data subject, can be described as data processing which is necessary to protect the legitimate interest of the controller[14.] This interest is the ability to prove fulfilment of the data subject's requirement and thereby fulfilment of Article 17 of the GDPR, and avoiding the risk of sanction[15] or other penalty. For this purpose, the processed data should be stored separately and the controller is required to ensure that they are not used for any other purpose. The data in the scope indicated above, stored for this purpose, for example as part of a log, cannot in themselves be a subject of a successful request for erasure if the legitimate interest of the controller

[13] Processing of personal data for marketing purposes is comprehensively discussed in Chapter C) 4.

14 For at least the time limit of the limitation, respectivelypreclusion period.

15 A fine of up to EUR 20 000 000 or 4 % of the total global annual turnover of the group for the preceding financial year can be imposed for a breach of the obligations laid down in Article 17 of the GDPR in accordance with Article 83 (5) (b) of the same regulation.

in their storage persists, as none of the cases provided for in Article 17 (1) of the GDPR relates to them.

A procedure can also be considered as acceptable by the legal regulation, where an irreversible erasure of all personal data happens, or an irreversible erasure of the data subject's identification data and the remaining personal data become anonymised as a result. The prerequisite for this is the fact that the controller has clearly defined internal policies on the erasure of identification data after the lapse of predefined periods. No GDPR provision implies a duty for the controller to prove the date of erasure of particular personal data (however, the controller may, of course, set up a solution that will enable this). Therefore, it should be sufficient for the controller in this case to be able to prove that it has set rules for the liquidation of all personal data or identification data, according to pre-defined periods, and that it does not maintain the data any longer (all personal data have been irrevocably erased) or that it does not process any remaining personal data otherwise, for which the prescribed period of their processing has already expired, or with regard to which it does not have the title to such processing.

Both options are possible. It always depends on the specific bank, the data controller, which of them it chooses, taking into regard its internal processes and the technical environment. However, the whole process must be described in internal regulations and documented.

✓ In which repositories must the data be immediately erased?

The erasure of data must be implemented primarily in actively used databases and systems. The obligation to immediately erase data does not have to be applied to the same extent to systems intended solely for storing the data; for such systems a flat erasure of data at predetermined periods is usually sufficient. In the case of data recovery from backups, it is consequently necessary to erase personal data if the purpose of their processing has expired.

✓ How should the right to erasure be implemented in the case of stored physical documentation?

In the case of physically stored documentation containing personal data, it is sufficient to adopt a procedure where the bank maintains, respectively archives, the contractual documentation of the particular client and proceeds to its shredding only after the expiration of the statutory period following the termination of the last similar product provided to that client.

1.3 The right to data portability

The right to portability is an entirely new right in the area of personal data protection. Portability means a transfer of certain data of the data subject from one service provider to another or to the data subject itself. One could say that the right to portability complements the already established right of access to personal data.

It follows from the GDPR that in order to enable the provision of data to a data subject, the following conditions must be cumulatively satisfied:

a) The processing is based on consent or a contract[16], and
b) The processing is carried out by automated means[17].

[16] Article 20 (1) point a) of the GDPR.
[17] Article 20 (1) point b) of the GDPR.

The form of data transferred

In accordance with the GDPR, the personal data transferred should be provided in a structured, commonly used and machine-readable format (for instance XML, CSV). This does not, however, mean that the new controller must accept the data from the original controller unreservedly, since the GDPR sets no obligation for the controller to process such data further. Even if the controller uses one of the commonly used and machine-readable formats, it does not have to automatically imply "data readability" for the data recipient/the new controller to which the data are transferred by the data subject. The subject should not have the right to choose how the data will be transferred to the new controller. It is up to the bank to take into account and decide on the way the data is provided and assess whether the transfer is technically feasible and safe. The fact that the bank chooses a safe and, at the same time, adequate means of communication, although different from those chosen by the client (for instance through an application developed for that purpose by a third-party) does not mean that the bank has failed to fulfil its obligation under Article 20 of the GDPR.

Scope of data provided by banks

Given the scale and sensitivity of information processed in the banking sector, including, among other things, banking secrecy, this right should be interpreted more widely. In certain cases, it is therefore also possible to request justification of a specific request from the data subject. The scope of the data should be limited only to the data of the data subject, the data subject has the right to freely dispose of his or her own personal data. Transferred should be the data that were actively provided by the data subject either through a written or web form for the purpose of concluding a contract for the provision of a product or service, or actively provided based on consent. The right should not be applied to data that the bank derives from the behaviour of the data subject. Such data can, for example, be payment transactions made by the client or information provided during a telephone call with the client. Transmission of such information under the right to portability would interfere with the rights of third parties. Banks consider it very problematic to provide data at the client's request to an unlimited extent, especially with regard to the scope of data processed by them. Too wide an interpretation of the right to portability would, moreover, be contrary to the purposes of the processing, as each controller may process only the necessary scope of data; this is why it is not appropriate, , for banks to provide, for example, data on payment transactions to telephone operators. Moreover, it is always necessary to make sure that the rights of third parties are not adversely affected when providing data and to take account of the obligation to ensure the security of the data provided, thus protecting the data subject at the same time.

Considering the scope of data processed, the banking sector must be used as a benchmark for data security, especially for ensuring very strong data security, both technically and organisationally. The GDPR does not provide the possibilities to review requests of the data subject and to request justification. It is in the interest of the data subject that banks interpret the right to data portability in a way that prevents confidential data, which is subject to bank secrecy, from being misused by a third party. Banks will only provide information within the financial sector that is not readily available to the data subject and that is aimed primarily at enabling it to negotiate a similar/comparable product with another financial institution. The GDPR is revising this interpretation to include also non-financial data and banks therefore believe that it should be only identification, contact, or possibly socio-demographic data that could help the data subject to apply for other than a banking product or service. The data subject may request a broader scope of personal data under the right of access to personal data and then freely dispose of a copy of the processed personal data received from the controller.

Authorization, not an obligation of the bank to receive data

The GDPR does not impose a direct obligation on data controllers to receive data from a data subject that it brings from a third party. As great emphasis is placed on the security of internal systems working with data in the banking environment, any transmission via a media from a third-party can pose a risk of threatening the bankenvironment with a virus or other malware. In particular, the right to portability should be fulfilled when using means under the Payment System Act. In other cases, the right to portability may be difficult to implement for security reasons.

Right to data portability vs.account switching in the banking environment

A special regulation of portability exists in the field of payment accounts in the banking environment, which is based on the Payment Services Directive, transposed in the Czech Republic by Act No. 370/2017, Coll., the Payment System Act (hereinafter referred to as the "ZPS")[18]. In this regard, the ZPS represents a special regulation which takes precedence over the GDPR when a request for a data transfer is made to another provider of the same service.

In the event that the rules for transferring the payment account (rules according to the GDPR vs. rules according to the ZPS) are set differently, they would be in conflict with the rules for changing the bank and with the rules of the new account information service contained in the Payment System Act, which sufficiently cover the purpose of the concept, i.e. facilitating sectoral mobility.

1.4 Right of access

In accordance with Article 15 of the GDPR, the data subject shall have the right of access to his/her personal data. The purpose of the right is to provide a possibility of finding out what the particular controller is processing about the data subject. The data subject finds out how the data is handled, which data the bank processes, both as the controller or processor, to whom the data can be provided, and from where they are obtained. This right is only activated after the data object lodges his/her request.

The form of information provided to the data subject

In accordance with Article 12 of the GDPR, it is essential to provide information in a concise, transparent, intelligible and easily accessible form, using clear and plain language. It follows from the above that the controller should collate information from the systems and provide it so that the data subject understands them. Information may be provided to the data subject both orally and in writing (physically on paper/electronically). Information provided electronically can be provided in the commonly used electronic format (for instance pdf, xls, etc.), it is at the discretion of the bank to decide whether or not to choose such format.

Ways of providing information

Each bank determines which is the safest way for it to communicate. An example of good practice can be provision of data to the internet banking mail-box of the data subject.

Content of the information being provided

The controller has a duty to provide the data subject with specific information on the processing of personal data, i.e. what personal data the controller is processing, the source they come from, for what purpose they are processed, for how long, whether they have been or could be made available

[18] Comp. Sections 203 – 209 of the ZPS.

to other subjects-recipients and others information referred to in Article 15 (1) GDPR. The scope of provided data will vary across the banking sector depending on the products negotiated. The aim of this right is to provide the data subject with comprehensive information on which data the bank processes. This means that the subject that uses its right of access should get an idea of what the bank is processing about him/her on the understanding that layering of information is not excluded. The controller should not have an unlimited obligation to provide the data subject with all personal data that it stores about him/her from the establishment of the contractual relationship at any time and under any condition. Banks are not obliged to provide the data subject with information that has already been provided to him/her or which is at his/her disposal. Typically, this can include, for example, transaction data in internet banking. The controller always informs the data subject of the purposes of the processing and of the data categories being processed.

Individual stages of executing the request:

a) Identification of the client

After the request is lodged, the GDPR requires the controller to identify the data subject. Recital 64 of the GDPR provides that the controller should use all reasonable measures to verify the identity of a data subject. The controller is obliged to disclose this fact to the data subject and enable him/her to prove his/her identity in a certain way (for instance by visiting a branch or by proving electronic identity). If the data subject refuses and does not repeatedly prove his/her identity in remote communication, the controller will not comply with the request. It is up to the controller to assess the level of verification that is sufficient for it, therefore it is not excluded to request, for example, an authenticated signature from a data subject, taking into account the form of communication and the nature of the data that the controller processes on the data subject.

b) Confirmation of personal data processed

The bank has a duty to disclose to the data subject whether or not it processes his/her personal data. After the confirmation, the bank is obliged to provide specific information on the processing without undue delay, usually within one month of lodging the request and in justified cases within 3 months at the latest. A justified case may occur, for example, when the controller needs third party cooperation (card association, etc.). Providing confirmation on the processing of personal data to the data subject together with providing specific information on the data subject is not excluded, of course under the condition that both actions occur without undue delay.

Possible action by banks when providing information to the data subject who uses the right of access to personal data (example of good practice):

- First, the bank provides a general framework including specific information, such as identification and contact details, a summary of the products provided, and other information that will describe the data that are available to the controller to the data subject. The aim is to provide comprehensive information on the current personal data to the data subject, taking into regard transparency, clarity and effectiveness of information provided.
- At this stage, the controller is not under an obligation to provide specific historical data to the data subject if the controller fulfils the information obligation to the data subject and the subject knows that they are available to the controller. The controller will alone determine whether and how it will provide the personal data to the data subject, taking into regard the scope of the services provided.
- Where the data subject is not satisfied with the data provided and where it will request specific information relating to a particular service, a particular purpose, or a particular category of data, the controller is obliged to provide him/her with such information. At this stage, it could be historical data (for example, the data subject may request information on payment cards issued for the entire duration of the contractual relationship).

Limits to the right of access to personal data

Just as every right has its limits, the right of access to personal data may also be limited. It may not be possible to provide the data subject with all the information. In this case, the controller will be able to provide the data subject with information explaining that the provision of personal data is not possible because it would involve a disproportionate effort by the controller[19]. Such disproportionate effort could, for example, be the provision of technical data on backup tapes with which active operations are no longer carried out, or it could be information when the interest of another person overrides the interest of the data subject. Furthermore, the refusal of information is not excluded if required by specific legal regulations which are accorded priority of application and impose a certain obligation on the bank (these could typically be prudential requirements resulting from the ZOB, AML, the Criminal Procedure Code, the Code of Civil Procedure, etc.).

Whereas the GDPR regards not only active activity related to data as processing, but also their storage, which means non-active processing, where the controller no longer actively uses personal data for its activity – the fulfilment of the contract - the law requires the controller to store personal data in the sense of temporary archiving (typically, this may include personal data stored by the controller in different repositories, such as backups, archives, tapes which are not actively used by the controller), it is necessary to determine the level of detail which will be provided to the data subject. Indeed, if this would in practice mean providing the data subject with all the information that the controller uses for no other reason but to comply with its legal obligations to store data, the controller would have to use disproportionate efforts to "revive" that historical data. Therefore, as long as the data subject does not reasonably require specific historical data, it is considered to be sufficient to provide actively used personal data.

2. Marketing

2.1 Direct marketing

Banks use different ways to reach out to clients. One of the main ways is the use of direct marketing, which, however, is not specifically defined in the GDPR, even though GDPR works with the term and understands such processing as processing carried out for legitimate interest in accordance with Article 6, Section 1, point f) of the GDPR. The GDPR, however, enables data subjects to object to such processing of personal data. In that case, the data subject's personal data will no longer be processed for the purposes of marketing. Data subjects can be approached if the interests of the controller do not override the interests or the fundamental rights and freedoms of the data subject.

a) Legitimate interest in direct marketing

Legitimate interests of the bank include, for example, a situation where there is a specific relationship between the controller of personal data and the data subject (typically the client's relationship with the bank).

Individual banks use different communication channels for the purposes of communication in connection with direct marketing, Typically, these include e-mail, short text messages (SMS), internet banking, personalized advertising banners, phone, push notification, and mail. In order to ensure the rights of the addressees, data subject has to be ableto use the possibility of making an objection against the legitimate interest in direct marketing in individual banks. Banks may use personal data known to them for the purposes of direct marketing, data which are published or otherwise freely

[19] Compare recital in Article 62 of the GDPR

available, for example, on the internet, if there is a connection between the purpose of the publication of data and the bank's offer.

It is not possible to use the objection against processing in the case of advertising banners in the banking environment (internet and mobile banking) which are not individualized (no segmentation or profiling are carried out) as when they are prepared, no processing of the personal data of the data subject is carried out. It is an advertising space with a non-personalized offer, which can be analogously compared to a poster in the premises of the bank's branch.

b) Expectability of marketing offers on the part of clients

All banks are business entities seeking to generate financial profits as part of their business activities. For this purpose, the client may be approached by the bank with offers of products and services of the bank, and may be approached by other businesses that are members of the financial group to which the bank belongs, without requiring his/her prior consent. Products of other businesses that are members of the group can also be offered by the bank itself. Typically, these are offers of other financial services provided by other group members, such as savings, insurance, investing, etc., or other payment services. Banks may use legitimate interest within the meaning of the GDPR to reach out to clients, but they can also approach clients in accordance with Act No. 480/2004 Coll., and Section 7. In this case, banks comply with the appropriate method of informing them of the reason of sending and the method of unsubscribing such offers. For more details, please see point 2.5.

2.2 Categorisation in direct marketing

a) Simple categorisation – legitimate interest

In the interest of objectivity, banks work with several types of categorization in direct marketing. In a simple categorization, banks work only with the basic identification and contact information, and a large group of clients can be approached this way. Sorting of the data subject takes place during processing - clients into certain target groups (selected, for example, in accordance with their specific place of residence, age, specific product, etc.). The client may also receive a product offer that is offered within a particular financial group.

b) Advanced categorization, or gross segmentation - legitimate interest

Banks use categorization of the data subject for their marketing activities, which enables them to better target a specific target group. Typically, this may include the processing of basic personal data of the data subject derived from the transaction history (for instance the data subject's summary of income and expenditure). For example, a specific offer may consist of offering a certain discount or reward to a particular client segment. Banks assume that clients expect to receive adequate service, for example by providing the client with an appropriate marketing offer based on selected client data. Banks, however, reflect clients' requests where the client does not wish such offers. An offer from another specific financial group entity can also be sent to the client within this categorization, if the expectable service is subject of the offer.

c) Profiling in marketing – consent

Banks process a large amount of personal data of individual clients in their activities. Typically, this may involve processing a different combination of the data of the client and indicators about him/her to create a profile with his/her preferences and anticipated needs. This kind of processing serves to better understand the client's behaviour and consequently to keep this information permanently above the particular client, not specific individual targeting. The processing of the client's personal data in this manner already requires the client's consent.

2.3 Pre-approved credit limits

One of the main activities of banks is to provide credit products. Such an offer is non-binding for the client and it merely indicates the client's possible credit options. Such an offer has no legal impact on the client. So-called pre-approved credit limits also serve to improve and speed up client service. In this case, it is not a marketing activity in the true sense of the word until the moment of a targeted communication of the pre-approved limit to the client, or of information derived therefrom.

2.4 Marketing surveys, customer satisfaction surveys

Banks seek to provide quality services to their customers and further improve their services in the course of their commercial activity. To this end, they can approach their clients with different surveys, typically with satisfaction surveys, surveys regarding the relevance of products offered, and surveys related to the development and preparation of new services. Banks can approach their clients with such surveys through e-mail, call centres, or other common communication tools. From this point of view, however, this is not a marketing activity in the true sense of the word, but a legitimate interest of the bank in not only improving its services, products, but also ascertaining interest in specific products, etc.

2.5 Commercial communication vs. servicing and technical messages

Further to the legislation mentioned above, the bank must also apply other legislation in certain forms of marketing messages (for instance e-mail, SMS), i.e. Act No. 480/2004 Coll., on Certain Information Society Services. A controller may disseminate commercial communications by electronic means in accordance with this legislation if, in the context of such an offer, the client may simply refuse the dissemination of such commercial communications. In addition, such commercial communication is properly identified by the words 'commercial communication' or 'CC', while the identity of the sender may not be concealed. Such commercial communication must also contain a valid address to which the addressee can send information that he/she does not wish to receive any further commercial communications or a different way must be indicated to unsubscribe from receiving future commercial communications. In the case of banks, such a commercial communication may, for example, be information about a new product that is sent to the portfolio of clients whose contact details are processed by the bank in relation to the products already in place.

Banks can nevertheless communicate with their clients not only via marketing communication or by sending a commercial communication, but they must, for instance, inform clients in selected cases about legal documents (change in product conditions, bank account statement, etc.). They may also inform clients that internet banking that is used by the client will be disabled or that it has been shut down due to a technical fault. Similarly, the client may be informed that a bank branch is closed due to a technical failure or reconstruction. In such cases, it is not a commercial communication within the meaning of Act No. 480/2004 Coll. These are technical and service messages that banks are obliged to send to their clients on account of fulfilment of their legal obligations or performance of the contract.

3. Information obligation

The data subject has the right to be provided with information defined in Article 13 of the GDPR, in a situation where personal data are obtained by the controller from him/her.

It is necessary to provide at least the identification of the controller, the contact details of the controller and of the controller's representative, the purposes of the processing for which the personal data are intended as well as the legal basis for the processing, in particular where the processing is intended to be based on legitimate interest as well as information regarding the recipients or categories of recipients of the personal data. Where the controller intends to transfer the data obtained to a third

country or international organisation, such communication must also be included in the information obligation, including the grounds for such transmission.

While providing this information, the principles of transparent communication, comprehensible form of language and legibility should be taken into account in particular. Therefore, it is appropriate to layer the volume of provided information, provide basic data in accordance with Article 13 (1) of the GDPR, while maintaining maximum transparency, and provide detailed information by reference or on another page. Supplementary information relates in particular to information pursuant to Article 13 (2) of the GDPR, i.e. to providing information on the obligation to provide the data and the consequences of not providing them, the period for which the personal data will be processed, the existence of the right to request access to and rectification, or erasure of the processed data, the existence of the right to withdraw consent or the right to lodge a complaint with a supervisory authority and, where appropriate, information on the existence of automated decision-making in accordance with Article 22 of the GDPR. Also, in the on-line environment, a gradual instruction as to the processing of personal data should be used where data subjects are informed about the processing of their data in multiple steps (this approach consists of providing key information in a short message with a link that will further expand each part of the instruction by providing a full version).

Information does not have to be provided to the data subject if the data subject has such information. It is sufficient to do so at the start of the negotiations, or if the controller obtains additional data, or for other purposes of which it has not yet informed.

If personal data are not obtained directly from the data subject, i.e. where the controller takes them over from another entity or controller, the information obligation must also be fulfilled, unless the data subject already has such information or where a disproportionate effort would have to be made to transmit such information. In justified cases, the information duty may be transferred to that other person (client), for example, informing an insured person different from the policy-holder.

Information obligation does not apply if the data are not obtained directly from the data subject, as a result of a statutory obligation, in the public interest (for example, security), or on the basis of laws - FATCA, AML, fraud prevention, while additional rules are provided for the protection of legitimate interests of data subjects (for instance, confidentiality).

4. Client – legal entity in relation to GDPR

In accordance with recital No. 14 of the GDPR, the GDPR does not apply to data of legal entities. Thus, the application of the GDPR had only a minimal impact on the processing of data relating directly to legal entities. Such data typically include the name (business name) of the corporation, the legal form, the address of its registered office or of the individual sites, as well as (working) contact details of natural persons (telephone, e-mail address, etc.) acting on behalf of the corporation.

However, when personal data relating directly to specific natural persons are processed in connection with servicing legal entities, the provisions of the GDPR have to be applied to processing as appropriate. An example of this procedure can be the processing of the address of permanent residence, private telephone number, number or copy of identification document, date of birth or birth number of the person. In such cases, the appropriate legal grounds for the processing should therefore be found for the processing in question and all other relevant rules for processing such data should be applied, in particular with regard to the legal grounds and purpose of further processing.

In this situation, the most frequent case is data on specific natural persons authorized to represent the client, whether data on members of statutory bodies of the given corporations, persons authorized to use accounts or otherwise communicate with regard to the fulfilment of the agreed product or

service, or to use payment cards. In such cases, it is necessary to process the personal data of those persons, in particular for the purpose of their proper identification.
The bank must therefore adequately meet the requirements of the GDPR in this respect, in particular minimize the amount of data processed, determine the periods of their processing, and provide for updating the data accordingly.

As regards performance of information obligation in these cases, it can be very impractical or even impossible. The bank should therefore inform the data subjects concerned of processing their data directly only if it is practically and effectively feasible. Conversely, if this is not effectively feasible (for example, where the personal data of the natural persons are collected and transferred to the bank directly by the given legal entity as data of its employees), the legal entity itself which transfers the data to the bank should inform the natural person about the data transfer accordingly (for example, this may be a transfer of data for the purpose of issuing, transferring and using a business credit card). At the same time, the inclusion of this procedure in a contract between the bank and the legal entity may be considered. Likewise, the obligation to update data on natural persons in a reasonable manner may be regulated in the same way.

The bank should inform the general public in a freely available and publicly declared information memorandum about the details of the processing of data of natural persons in connection with the servicing of clients - legal entities.

Specific cases of processing, such as data on the ultimate owners of legal entities processed for the purposes of the AML Act, or the storage of data on executed transactions for the purposes of the fulfilment of the ZoB, can be performed on the legal basis of fulfilment of legal obligation. Therefore, such processing does not need to be specified in more detail and the data subjects of the processing do not have to be informed.

In relation to clients - legal entities, a number of cases occur in practice, where these clients request that the transfers of personal data of their employees, carried out by means of current payments (for example, payment of wages, reimbursement of costs incurred during business trips, etc.), be anchored in a processing contract concluded with the bank in which the bank would be in the role of a data processor. In this respect, however, it is true that although banks, while providing their product, comply with the instructions given by the client, thus executing the transactions in question, taking into account the specific legal regulation of the provision of the product (ZPS, ZoB), are not in the position of a data processor performing the processing of personal data for the data controller, the client. In these cases, therefore, there is no need to conclude a specific contract or an amendment pertaining to the processing of personal data beyond the framework of the existing contractual relations.

D) SPECIFIC RULES FOR PROCESSING PERSONAL DATA OF BANK EMPLOYEES

In order to provide for the stability of the bank and in view of the interconnectedness of the banking sector, and thus also the stability of this segment of the national economy as such, the bank is required to act with prudence, to identify and manage the risks it may face in its activity, and implement an adequate internal control system.

Detailed requirements for managing risks and for the bank's management and control system are laid down in particular by the ZoB and in the so-called prudential decree, i.e. the Decree of the Czech National Bank No. 163/2014, Coll., on the performance of the activities of banks, credit unions and investment firms, as amended. The question of employees' reliability as an integral part of the overall system is regulated particularly in Section 17 (3) and (4) of the prudential decree. The bank is required by these provisions to establish in particular the principles of human resources management, including staff recruitment principles, including the setting and application of specific rules to verify the trustworthiness of employees and members of bodies.

The requirement for the trustworthiness of employees is also formulated in other regulations that regulate some of the products provided by the bank. These include, for example, Section 72 of the ZSÚ or Section 14a of the ZPKT, which both require the bank to ensure that its employees participating in the provision of the product, are trustworthy.

Based on the sectoral regulation and the object of its activity, the bank is therefore required to lay down rules to verify the trustworthiness of its employees, not only to demonstrate fulfilment of its legal obligations, but also to protect its legitimate interests, such as, in particular, protection of the bank's assets and its clients.

In order to protect the interests mentioned above, trustworthiness has to be verified both during the recruitment selection procedure to fill the post and during the employment relationship. For certain job positions, a thorough assessment of the integrity of the applicant is directly imposed by a special legal regulation[20], while in other cases it is possible to do so in order to secure the legitimate interests of the bank and of other persons, taking into consideration any specific circumstances. In the latter case, it is up to the particular bank to assess the risk associated with the job and to decide which personal data it considers necessary to verify the trustworthiness of the employee, or job applicant. Such an assessment is also the proportionality test as defined in Article 6 of the GDPR, in which the bank considers its interests and the interests of its clients and, on the other hand, the rights to protect privacy of the persons concerned.

Among the facts that usually have to be assessed when reviewing the level of risk of a job, respectively when performing the proportionality test, are in particular:

- The subject of the employee's work activities and its relationship with other internal processes of the bank
- The scope of access to confidential information
- The ability to assist unauthorised manipulation with the assets of the bank or of its clients, directly or indirectly
- The quality and functionality of automatically performed checks of the employee's activity
- The strength and parameters of the bank's other internal controls

Personal data can be processed to a reasonable extent to verify the trustworthiness of the employee or job applicant based on the risk assessment and the performed proportionality test. The legal title

[20] For instance, in the case of natural persons involved in the provision of consumer credit, for which the obligation to verify their credibility is regulated in Section 72 of the ZSÚ.

for such processing is the legitimate interest in accordance with Article 6, Section 1, Point f) of the GDPR.

Personal data can in principle be obtained from three sources: from employee or job applicant, from public sources (Trade Licensing Register, Insolvency Register, Central Register of Executions, other publicly accessible data) and from other data controllers who can confirm the accuracy of information provided by the employee or a job applicant, and have sufficient legal grounds for this, such as the previous employer, school or certification authority, the certificate of which should be at the disposal of the employee or the job applicant. The legal title of the legitimate interest can generally be used to collect and further process personal data from all types of sources. The employee's consent will be required only for the provision of information if explicitly required by a special legal regulation, such as Section 314 (2) of Act No. 262/2006 Coll., the Labour Code.

E) AUTOMATED INDIVIDUAL DECISION MAKING, INCLUDING PROFILING

In connection with the need to process large amounts of personal data, which occurs in the provision of banking services, **new fully automated procedures for more efficient provision of financial services and proper compliance with regulatory obligations are also being developed and established**. Due to the scope of processing of personal data and the complexity of calculations in such processing, processes based on automated decision-making (including profiling) are often introduced **primarily with the aim of ensuring consistency and correctness of outputs,** for example in risk management, to reduce the likelihood of human error or to prevent fraudulent behaviour.

In the area of customer service itself and the related provision of products and services, automated decision-making enables banks to accelerate and increase the overall efficiency of the process of servicing the client, which above all benefits the client. For example, in a fully automated process, the system can decide on an application for a loan (in particular consumer loan), or a mortgage credit (including setting up the applicant's risk profile) without human intervention, or, for instance, on setting up an investment profile when concluding investment products, or detect fraudulous behaviour without human intervention in the electronic channels environment, etc.

The input for the automated decision may be personal data provided directly by the data subject (for instance, identification and contact details) and personal data obtained from a third party (for instance, from the credit register), as well as derived or inferred data relating to the data subject (for example, the risk profile of the client). **Automated decisions can be taken using profiling, or without it; thus, profiling can be performed without automated decision-making and these two are not necessarily interlinked activities.**

Automated individual decision-making must be based solely on automated processing, hence the relevant provisions of the GDPR[21] do not apply to decision-making which is based only on partially automated processing. This does not apply if the involvement of the human factor is merely formal in a part of the decision-making process, without a logical influence on the outcome of the decision-making.

[21] In particular Article 22 of the GDPR.

The appropriate **legal grounds for automated decision-making (including profiling) are**:

- **Consent of the client,**
- **Conclusion or performance of a contract to which the data subject** (client of the bank) **is party**
- **Requirements of the Union law or Member State law**.

Taking into regard a possible future need to demonstrate the lawfulness of automated decision-making (including profiling), for instance to a supervisory authority, the controller is certainly advised to proceed in a way enabling it to be able to demonstrate the existence of proper legal grounds for processing at all times of the processing.

Automated decision-making (including profiling) can be performed if the following conditions are cumulatively met:

a) The data subject has been made aware, by means of a document describing the conditions of the protection of privacy, **of the existence of automated decision-making** (including profiling), including the procedure applied, and of the possible consequences of such processing for the data subject.

The fulfilment of this condition should not adversely affect the bank's rights, for example where the disclosure of detailed information about the procedure used in automated decision-making may constitute conduct that could jeopardize or violate business secrets or jeopardize its fraud prevention measures.

It is recommended to assess whether the data subject should not be informed when personal data are entered in the process itself (for instance, information that the process is automated decision-making, is clearly indicated in the loan application form that the client fills in the electronic channel environment) before personal data are processed in the automated decision-making process.

b) The controller is obliged to enable the data subject to exercise his/her rights, namely

- The right to human intervention on the part of the controller,
- The right to express his or her point of view,
- The right to challenge the decision reached as a result of automated decision-making (including profiling).

Pursuant to Article 22 of the GDPR, the bank's client (a natural person, data subject) has **the right not to be subject to a decision based solely on automated processing, including profiling,** which produces **legal effects concerning him or her or similarly significantly affects him or her**. A typical legal effect is the creation, change or termination of a contractual relationship.

However, it is not the duty of the bank as the controller to enable the data subject **not to be subject to automated decision-making (including profiling) where the data subject requests manual processing already at the start of the process** (for instance, when a loan applicant requests that the application be reviewed exclusively by manual means). The reason is to maintain a consistent and transparent approach to all data subjects and to ensure the speed and efficiency of the process. This is without prejudice to the right of the data subject to object to the decision made as a result of automated decision-making (including profiling) and to request a manual review.

In view of the fact that automated decision-making is based on a systematic and extensive evaluation of personal aspects relating to natural persons, which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning natural persons or

similarly significantly affect the natural person, the controller has a duty, when preparing such processing or a new process, to

c) Properly assess the impact of the automated decision-making on the protection of personal data (the DPIA)

d) Comply with other obligations for the proper processing of personal data as laid down in the GDPR, in particular to **ensure appropriate technical and organizational measures to protect personal data against breaches of their security, confidentiality or integrity**.

It is fully under the responsibility of each controller to select the tools and procedures that it will use to process personal data, but it should be mentioned that when implementing an automated processing process (and then throughout the existence of the process), the controller must be able to demonstrate that the method of processing is adequate with regard to the purpose of the processing and the nature of the personal data, and that the same result could not be achieved in terms of the privacy of the data subject by less invasive procedures/methods, i.e. that automated decision-making is an appropriate procedure.

In view of the impact of automated decision-making on the data subject, it is necessary that the **processes that are based on this method of personal data processing are subject to periodic reviews and testing to ensure their accuracy and effectiveness**. Banks are obliged to implement such technical and organizational measures to minimize the risk of errors in the processing of personal data in automated decision-making and secure such personal data in a way that takes into account the potential risks to the interests and rights of the data subject.

F) RELATIONSHIP WITH THE SUPERVISORY AUTHORITY

Data breaches

Banks have set up a number of processes in the area of information security and have tools in place to prevent, identify and address security incidents. The GDPR[22], like certain other regulations, requires banks to notify certain types of security incidents to the supervisory authority, the Office for Personal Data Protection (hereinafter referred to as the "ÚOOÚ"), and in certain cases directly to the persons concerned.

- ✓ In order to assess whether a particular security incident corresponds to the definition of personal data breach in accordance with the GDPR[23], account should be taken of whether it related to personal data processed by the bank, be it data of clients, employees or other persons, and whether a data security breach actually occurred.

A breach as defined in the definition mentioned above is not a security incident that may cause a breach of security of the personal data being processed, but only a real incident resulting in the above-mentioned consequences, i.e. interference with confidentiality, integrity or availability of personal data. Therefore, a security breach would not be a situation where a security defect was identified that could only potentially lead to an unlawful disclosure of data. A violation would happen where, for example, a genuine abuse of a weakly protected employee's mobile phone occurred, which would result in the above consequences.

[22] ZPS, the Act on Cyber Security
[23] Article 4, Section 12 of the GDPR

- ✓ Article 33 (1) of the GDPR connects the point in time where the period for a notification of a personal data breach starts to run with the moment when the controller, i.e. the bank, becomes aware of the breach.

A data security breach, or a suspicion of a security incident, can in practice be identified by a large number of employees - a branch employee (a banker), an employee in the marketing department at the Headquarters, Security, an IT Security Officer, Compliance, Anti-Fraud, Archive, etc. The types of cases would be widely different (lost or stolen documentation, forcible entry into the archives, mistakenly sent information to an unauthorized recipient, external intervention in the system, technical error of an application, etc.), just as the qualification of the employee would differ in terms of assessing whether or not to escalate the incident further.

It is therefore possible to conclude that the designation of the person (s) responsible for assessing security incidents and for setting up the overall process when each employee who can identify evidence or an event indicating a data security breach knows who to contact with this information, is crucial for the fulfilment of obligations imposed in this area by the GDPR on banks.

The start of the period, according to the wording and purpose of the given provision of the GDPR, should therefore be linked to a moment when the appointed employee has or should have sufficient information to establish with a high degree of probability that a breach of personal data occurred. This does not mean, however, that the start of the period runs only from the moment when the controller or processor, or the appointed employee have all the information about the incident. Collection of all information should be part of the investigation. An initial assessment of whether a security incident has occurred with a high degree of probability is therefore crucial for ascertaining the point in time when the period begins running. If the data controller concludes that this could indeed be the case, the 72-hour deadline for notifying a personal data breach starts to run. The complexity of a particular case may have an impact on whether notification is made within a given deadline, or later. Similarly, the beginning of the period may also be inferred for the notification of the event to the persons concerned as well.

- ✓ Assessment of security incident

It follows from the wording of Articles 33 and 34 of the GDPR that there are three possible procedures in the event of an incident being detected, according to its severity, or the level of risk for the rights and freedoms of natural persons:

a) The incident is unlikely to result in a risk to the rights and freedoms of the persons concerned. Therefore, it does not need to be notified to the supervisory authority or to the persons concerned. However, these incidents must also be registered internally.

b) The incident is likely to result in a risk to the rights and freedoms of the persons concerned, however, no high risk is involved. The prerequisite for reporting is that there is a real threat of harm or that harm will occur. Such an incident must be reported to the supervisory authority. A failure of the security feature itself, as well as an unsuccessful attack, are not subject to the reporting obligation in accordance with the GDPR.

c) The incident is likely to result in a high risk to the rights and freedoms of the persons concerned. An incident of this kind shall be notified to both the supervisory authority and the persons concerned unless any of the exemptions under Article 34 (3) of the GDPR apply.

In particular, the type and severity of the risk to the person concerned, the type of personal data breach, the nature, sensitivity and scope of the data, the categories of persons concerned, the ease of identification of persons whose data has been affected by the data breach, of the unauthorized

recipient and the number of persons concerned, shall be taken into account as decisive for assessing the level of risk. Development of an internal methodology describing how and by what criteria individual cases of personal data breaches are assessed **can be described as an example of good practice**.

G) PERSONAL DATA SHARING

1. Client registers

Banks share the necessary personal data with respect to individuals, loan applicants among themselves in order to verify the financial standing and creditworthiness of the loan applicant. Sharing can also take place with other non-bank entities which pursue the same purpose (verification of the trustworthiness and payment discipline of the applicants for a service). The sharing of personal data for the purpose described above occurs through so-called client registers.

The legislative framework for the functioning of client registries in the Czech Republic is defined by the concurrent existence of several legal regulations (ZoB, ZSÚ, the Consumer Protection Act), which regulate the basic rules in a different manner and whose relationship cannot be unequivocally determined.

As a result of this fragmented and inconsistent legal framework, the functioning of individual client registers used by banks to verify the financial standing and creditworthiness of the loan applicant (natural person) differs and is based on different legal titles.

a) Banking and Non-banking Client Information Registers

CBCB – Czech Banking Credit Bureau

The legal title for the processing of personal data and information on all relevant banking products in the CBCB's register is the fulfilment of the legal obligation of the data controller, based primarily on the ZoB and the ZSÚ.

CNCB – Czech Non-banking Credit Bureau

The legal title for the processing of personal data is the fulfilment of the legal obligation of the user of the register, resulting in particular from the Consumer Credit Act, as well as from other legislation governing the requirement to verify the creditworthiness of the applicant for a financial product and to prevent his/her over-indebtedness.

For the processing of personal data related to the provision of other than consumer loans to individuals, the legal title is the legitimate interest of the users of the register.

In the case of natural persons who represent a legal entity, have an ownership interest in it, or have another relation to the credit product applied for by the legal entity, the legal title for verifying their creditworthiness and trustworthiness title is consent.

Data sharing between CBCB and CNCB registers

From the perspective of banks, the legal title is fulfilment of the obligations of the controller, resulting in particular from the ZoB and the ZSÚ.

b) Solus registers

Negative registers of the Solus Association (Register of Natural Persons and Register of Legal Entities and Entrepreneurs)

The legal title for the processing of personal data is the legitimate interest of the controller in accordance with the Consumer Protection Act.[24]

Positive register of the Solus Association

The legal title for the processing of personal data is the consent of the data subject in accordance with the Consumer Protection Act.[25]

Detailed rules are provided in documents through which individual client registers fulfil their information duty. **An example of good practice is a** procedure whereby banks inform their clients and applicants for credit products at least in a general manner about the processing of their data in client registers (for instance in the form of an information memorandum) and refer to disclosure documents of the relevant registers for details.

2. Cooperation in commercial representation (mediation)

Financial institutions across the financial market work together both in order to be able to reach out to the widest possible group of potential clients as well as to offer their clients the most complete product offer possible.

In the context of cooperation in mediation, the following two basic scenarios can occur:

a) Sales representatives of banks

These are situations where the bank's products are distributed by their sales representatives. These can be both natural persons and legal entities (typically brokerage firms).

b) Bank in the position of a sales representative

These are situations where a bank distributes products of a partner company (typically, for instance, insurance products, supplementary pension savings, building savings, investment, etc.).

Distribution relationships in the context of the principles of personal data processing

In both of the above cases, the controller of personal data is primarily the entity that provides the product (in the case of point (a), the bank, in the case of point (b) an insurance company, a pension company, a building society, an investment company, etc.) and a sales representative, acting on behalf of the controller, is in the position of the processor of personal data.

In parallel, however, the sales representative may be in the position of the controller of personal data with respect to the same personal data, especially if the processing has a different purpose and the personal data in question:

a) Have to be processed by it in order to fulfil its statutory obligation resulting, in particular, from the regulation of the distribution of financial products,

[24] Section20za Paragraph 1 of the Consumer Protection Act.
[25] Section 20za Paragraph 6 of the Consumer Protection Act.

b) If it is authorized to process them for its own purposes if the client has given consent (for instance, for marketing purposes)
c) If it is obliged to process them for the purpose of performance of the contract with the client
d) If it processes them based on its legitimate interest (for instance, for the purposes of direct marketing based on legitimate interest).

In other words, a sales representative is in the position of the processor of personal data whenever it acts on behalf of a financial institution (typically, acts such as contract negotiation, contract conclusion, customer service in connection with the contract) and in other cases (for instance in connection with the fulfilment of obligations arising for it as consumer credit intermediary from the ZSÚ), it is in position of personal data controller.

In certain cases, even both subjects within the commercial representation may be controllers of personal data. Such a situation applies, for example, to the activity of so-called "tipsters", i.e. persons, who are not authorised to mediate financial products themselves, but can only ascertain the interest of a particular person in a financial product and pass this information and his/her contact details on to the bank selected by him/her.