ČESKÁ CZECH
BANKOVNÍ BANKING
ASOCIACE ASSOCIATION

FRAMEWORK INTERPRETATION OF CERTAIN GDPR PROVISIONS IN THE BANKING SECTOR

Prague, I March 2019

Update: June 2022

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, repealing Directive 95/46/EC (General Data Protection Regulation, hereinafter the "GDPR"), in the processes of providing banking products and services, taking into account the specificities of the banking sector and its dependence on the processing of personal data on a large scale. The aim of the document is therefore to lay down the interpretative framework for the banking sector used in the application of the GDPR with a view to ensure compliance with other financial market regulations and at the same time taking into account the specifics 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 to 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.

Banks are bound in their business by extensive regulation in all areas of providing banking products and financial services. In relation to natural persons, this includes, in particular, the implementation of the requirements of directly effective European regulations or directives transposed into the legal order of the Czech Republic, for instance, the Act on Banks, the Consumer Credit Act, the Act on Selected Measures against Legitimization 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 interested in their products and services, 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) mostly on the following legal bases:

- The processing of personal data is necessary for the conclusion of a contract and for 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 a change of the surname, updating contact details, etc.
- Personal data are processed based on the legal obligation imposed on banks by a binding legal regulation (Article 6 of the GDPR, paragraph 1 (c); this includes, for instance, data obtained from clients of banks in connection with mandatory measures aimed against the legitimization of proceeds of crime or data relating to credit exposure and payment behavior when negotiating consumer credit, etc.[1];
- Banks may process data based on their legitimate interest - this legal basis is balanced by the extensive rights of the data subject (Article 6 of the GDPR, paragraph 1 (f); this includes, for instance, sending direct 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

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

the conditions laid down in the GDPR (Articles 7 and 4 – the consent is verifiable, informed, 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.

Marginally, in specific cases, personal data processing may be necessary in order to protect the vital interests of clients (Article 6 of the GDPR, paragraph 1 (d), or for the performance of a task carried out in the public interest (Article 6 of the GDPR, Section 1 (e), for instance in connection with fight against pandemic declared by the government.

SPECIFICS OF CERTAIN LEGAL BASIS 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 of the bank, 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 generally consists of three basic parts:

- Defining the legitimate interest;
- Establishing that the personal data processing in question is necessary for achieving the legitimate interest;
- Assessing the alleged legitimate interest against the interests and fundamental freedoms 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 under 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 to the processing of personal data at any time on the basis of a legitimate interest on grounds relating to his or her particular situation,[2] (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 below in more detail). After receiving the request, the bank may therefore ask the

[2] And also, public interest.

data subject to describe the reasons raised by him/her in the objection, relating to his or her particular situation, which make him/her believe that the bank has no prevailing legitimate interest in the processing of his or her personal data.

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 contested purpose of the processing; the bank may thus 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 defense 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 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 this right should be presented clearly and separately from any other information at the time of the 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 (including, for instance, information on the processing of personal data published on the bank's web page) provided that the text is clearly separated from other information, for instance contractual information.

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

Banks generally use consent in connection with the marketing processing of personal data unless the marketing is based on a legitimate interest. In other cases when the consent with the processing of personal data is used, specific needs of individual banks are involved.

2.1 GDPR Consent

a) The basic rules for obtaining consents to the processing of personal data are:

- 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 provide 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 requested to express disagreement but only to express consent, since the GDPR knows only consent expressed by active conduct, not disagreement (i.e., the consent must be based on the *opt-in principle*).

- Consent does not have to be expressed on a separate form and may be part of another document, but it must be distinguishable from the rest of the text and the data subject must be able to indicate his or her willingness to give consent (for instance, by ticking a tick 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),
  - The domestic 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 on the right of the data subject to withdraw his/her consent, or the right to lodge objection to automated decision-making (comment, manual review, the right to challenge the decision), if it is performed on the basis of consent.

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

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 have to operate in a manner preventing 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 (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and Directives 2009/138/EC and Directive (EU) 2013/36, which has been implemented in Act No. 253/2008 Coll., on Certain Measures Against Money Laundering and Terrorist Financing, as amended (hereinafter referred to as the "AML Act"), whose application is further refined by the methodological instructions of the Financial Analytical Office of the Ministry of Finance of the Czech Republic (hereinafter FAU).

The main principle of this activity is to identify all persons connected with the banking product or service. For this purpose, banks ("obligated persons") carry out identification of persons, inter alia, by being allowed to make copies or extracts from the submitted documents and process the information so obtained if required by the AML Law or if necessary to achieve its purpose. In this case, the client's

written consent to make a copy of the document is not required but the client must be informed of the copying. If the customer expresses his/her disagreement with making a copy, the bank may only make an extract of the identity document, and only to the extent of the data necessary to achieve the AML purpose. The bank may make the provision of a copy of the identity document a condition for the provision of the service, taking into account the overall risk profile of the customer. Banks shall comply with the methodological guidelines and recommendations of the FAU.

If the document from which the copy is made contains data that are not necessary for the AML purpose (older versions of documents, data provided voluntarily – for instance, the marital status), these data are not processed systemically and their occurrence is random; it is permitted to leave such data on the copy in view of the integrity of the copy being made and the technical difficulty of masking selected data (various document templates),

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 check of the client 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, establishing a business relationship with a politically exposed person or a client established in a high-risk country.

In the event that the bank, in its activities resulting from the AML legislation, makes copies of the documents submitted during the identification or check of the client, it is required to store them for a period of 10 years from the transaction or from the termination of the business relationship with the client. The client does not give consent to the storing of 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 obligated person. After this period, the competent controller shall ensure the deletion of the data retained and the destruction of the documents, unless there is another legal title for the retention of the data and documents. The bank shall ensure a high level of security of access to the stored copies of documents throughout the processing period (access rights management, access logging) by appropriate technical and organizational measures.

b) Processing of the personal identification number

The processing of the personal identification number is governed by Act No. 133/2000, Coll., on registry books and personal identification numbers and on amending certain laws, as amended. This act exhaustively 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 Act No. 21/1992, Coll., the Act on Banks, as amended (hereinafter the "ZoB"), 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 identification data of the client in Section 5, which, inter alia, relates to the personal identification number, if allocated, as one of the basic identification data.

For the above reason, banks do not request consent from their clients or from other persons whose data they process in bank transactions based on the fulfilment of their legal duties, they do not request consent to process the personal identification number.

INTERNAL OBLIGATIONS OF BANK

1. Position, role and activities of the Data Protection Officer (DPO)

Basic requirements for the position, role and activities of the DPO are based on Section 4, Articles 37-39 of the GDPR. In particular, banks are required to appoint a DPO pursuant to Article 37(1)(b) of the GDPR.

The DPO's position within the organization must be independent, which is achieved in particular by:

- Clearly defining the position of the DPO in the hierarchy of the organization with a direct link to the top management level (usually the 1st or 2nd management level below the Board of Directors, “B-1” or “B-2”),
- Placing the DPO in the controlling (supervisory) structure of the organization, which is not directly involved in the performance of the bank's operational activities, up to the level of the member of the top management to whom the DPO reports (the “2nd Line of Defense”).

The role of the DPO should be established as a stand-alone role, not combined with the performance of other activities. The DPO position can be established entirely separately as, for instance, a "DPO Office" or within a broader unit structure, for instance Compliance or Legal Support. To avoid conflicts of interest, the DPO position cannot be created in departments that are directly involved in the implementation of data protection measures or data processing, such as IT, Human Resources, Client Transaction Processing, etc.

In order to ensure a uniform approach to data subjects and the efficiency of the DPO's activities, the DPO may exercise his/her powers throughout the Bank's group of entities that provide services mainly to retail clients. The DPO's activities within the group are then carried out on the basis of outsourcing contracts.

Taking into account the size of the bank or the group and the scope of its activities, the controller must ensure sufficient resources for the performance of the DPO's activities, in particular sufficient and specifically defined staff capacity.

In the context of his/her activities, the DPO:

- Provides advice (consultation) on the performance of processing activities at the request of the controller's functions, for instance, with regard to determining the appropriate legal titles for processing under Article 6 of the GDPR, etc.
- The DPO may be entrusted with keeping records of processing, but is not responsible for the completeness of the records of the controller's processing activities (the obligation and responsibility for notifying the DPO of all processing carried out rests with the owners of such processing in the bank's operational functions).
- Issues an opinion on the conclusions of the Data Protection Impact Assessment (DPIA) prepared by the controller, but does not approve the Assessment.

- Comments on the results of the proportionality tests upon request, but does not prepare or approve them.
- Issues opinions and methodological guidance on the application of data protection in the performance of the activities of the controller.
- Carries out his/her own controlling and monitoring activities to satisfy himself/herself that the controller's activities comply with the GDPR. As part of this control, he/she is not subject to the orders of other functions of the controller or the bank's management, but sets his/her own plan and procedures for controlling activities.
- He/she shall regularly, at least once a year or as required, inform the bank's senior management of compliance of the controller's performance with the GDPR and the results of the controlling activities. In this context, he/she may submit a summary annual report to the senior management on compliance of the controller's activities with the requirements of the GDPR.
- He/she may participate in assessing the risks and impacts of personal data breaches identified by the controller, in particular with regard to assessing the level of risk requiring notification to the Office for Personal Data Protection (hereinafter the " UOOU ") or notification to affected data subjects.
- He/she may participate in raising awareness and training of the controller's staff in the area of personal data protection, for instance by participating in the preparation of training materials, providing training, etc. However, the DPO is not responsible for the training plan and its implementation.
- He/she acts as a contact point for data subjects.
- He/she acts as a contact point for the UOOU.

In order to ensure that the DPO maintains expertise in data protection law and practice, the controller must ensure that sufficient resources are available for the training of the DPO and appointed data protection specialists, in particular through participation in professional conferences and seminars. It is also good practice to provide certification of knowledge for the performance of the DPO function (for instance IAPP).

2. Records of processing activities

The bank, both as the controller and the processor of personal data, is obliged to keep records of processing activities. The basic content of 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 are performed by it as the processor.

In practice, there may be situations where the bank is generally in the position of the controller of personal data but at the same time, it also performs certain processing for another controller, and in relation to these processing activities and personal data, it is then at the same time in the position of the processor (for instance, when providing outsourcing services within the financial group). In this case, one record of processing activities may be drawn while both roles of the bank must be stated in the record-keeping instrument and they must be distinguishable.

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 of contents contain at least information specified in Article 30 (1) of the GDPR where the bank is the controller, or in Article 30 (2) of the GDPR, if the bank is the 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 are personal data 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 standards.

Preparation and reviews of records of processing activities

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

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 described 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 breaking down 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 according to 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.

3. Data protection impact assessment

The assessment of the impact on personal data protection is also often known as the DPIA, the English acronym for the data protection impact assessment and is a means to manage the risks associated with the processes of personal data processing 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, particularly based on:

a. Account is taken of the cases which make it necessary to prepare the Assessment as contained in Article 35 (3) of GDPR;
b. Make a check to establish whether the processing is included or not in the types of operations that are not subject to the assessment, published by the UOOU[3];
c. Evaluation of the criteria listed in the list of types of processing operations that are subject to the data protection impact assessment published by UOOU [4].

It is not necessary to perform the DPIA if:

[3] The list of the types of operations that are (are not) subject to the data protection impact assessment requirement. Updated version 1.0 is available at https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=38940. The list is subject to the approval of the European Data Protection Board and may be subject to certain changes.
[4] ditto

a. The nature, scope, context and purpose of the processing are very similar to the processing for which the DPIA has already been carried out by the bank;
b. The processing operation was reviewed by the UOOU prior to 25 May 2018 under specific conditions and parameters of the processing which have not changed since then;
c. The processing has a legal basis in EU or Member State law where that law governs the specific processing operation and where a DPIA has already been carried out in connection with the adoption of that legal basis, unless the Member State has declared that it considers it necessary to carry out such a DPIA prior to the processing activities;
d. Legal regulation imposes an obligation on the bank to carry out specific processing of personal data (Article 10 of Act No. 110/2019 Coll., on personal data processing).

In the event that it has been assessed that a DPIA is necessary, the bank shall proceed in accordance with the methodology issued by the UOOU[5], or similar methodology, and shall carry out at least:

a. A systematic description of the intended processing operations, based in principle on the records of processing activities, or containing a diagram (workflow) describing the processing (flow) of personal data, including any links to other personal data processing, and identifying the agendas and departments responsible for the processing personal data;
b. An assessment of the necessity and proportionality of the processing operations in relation to the purposes through a proportionality test;
c. An assessment of the risks to the rights and freedoms of data subjects, in which the bank follows a general risk analysis[6] to ensure consistency of the measures taken, in which the bank identifies the primary and supporting assets, their vulnerabilities and the resulting threats; and
d. A description of the measures planned to address those risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR, and a determination of the level of residual risk once the identified measures have been implemented.

If the level of residual risk (below the level of 48 according to the UOOU methodology) cannot be sufficiently reduced, the bank must initiate prior consultation with the UOOU.

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 online platform);
- Introduction of a new automated scoring process for clients;
- Introduction of an entirely new product.

Where appropriate, the bank will engage the relevant third parties, possibly including data subjects, or their representatives, in the process of the DPIA described above, in the form of consultations.

The resulting impact assessment, including acceptance of residual risk, shall be approved by a responsible person appointed by the operator, different from the DPO.

Banks are not required to publish DPIA results. A DPIA is not a one-time process, and the bank therefore periodically, or in cases of extraordinary events, reviews compliance with DPIA's findings within the

[5] Methodology of general assessment of impact on personal data protection, Version 1.0 dated 11 November 2020 available at https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=46487

[6] See, for instance, obligation under Act No. 181/2014, Coll., the Act on Cyber Security, as amended, if the obligations in question apply to the bank.

established processes and verifies whether there has been a change in input parameters or risks that would justify a review of the current process and possibly launch of a new DPIA process, including reviews of requirements for preparing a DPIA (applicability of exemption, etc.).

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 (in accordance with the list issued by the UOOU), development of the DPIA itself and of its life cycle, can be described as an example of good practice.

4. Data retention (archiving) period

(For the purposes of this document, the start of the retention period after the phase of active processing of data within the service provided is usually the moment of termination of the contract, i.e., the individual banking transaction, between the bank and the client. However, given the scope of the data processed and the complexity of banks' information systems, the start of the data retention period may in some cases be determined by the termination of the relationship with the client, i.e., all of the client's contracts.)

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

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) The Act on Banks (hereinafter the "ZoB"), which provides, in particular, for the obligation to process personal data necessary to execute the trade and assess the risks;
   b) The AML law, 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., the Act on Business Activities on the Capital Market (hereinafter referred to as "ZPKT") relating in particular to communications records and documents relating to the investment service provided;
   d) Act No. 499/2004 Coll., the Act on Archives and Records Service, as amended, relating to the retention of personal data for archival purposes.

   The Act on Banks stipulates the obligation to retain data about transactions that have been carried out for 10 years after their completion. This period can thus be considered as a basic period for all interactions of the bank with its clients with regard to the transactions executed.

II. Processing required for the purposes of the legitimate interests of banks, 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). The appropriateness of this time limit shall be assessed by the bank in the context of proportionality tests, ideally at the level of individual categories of banking transactions, also taking into account the likelihood and consequences of such intentional behavior and the realistic time horizon needed for their detection.

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

The limitation periods of offenses 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 for which the bank has to keep the data in order to protect its rights. For the purposes of proving that no misdemeanor 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 a particular case. The limitation period for misdemeanors arising from ZoB, AML and ZPKT, is 3 years (Act No. 250/2016 Coll., on Liability for Misdemeanors 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.) The application of a specific reasonable period of time must reflect the likelihood and actually observed events relevant to the assessment of the purpose in that period and to the type of activity of the bank.

Taking into consideration the fact that the management of retention periods and subsequent deletion/anonymization of data are generally provided by system batch processes, it is reasonable for the baseline period derived from the above assumptions to be extended by up to 1 year. Likewise, in cases where the limitation period may be suspended, it may be in the interest of the bank to retain personal data in certain cases for additional 2 years beyond the 15-year period, following the completion of the transaction to prevent lack of evidence in the event of litigation. In our experience in court practice, the bank may not be aware that any proceedings have already been initiated against it - it is a common court practice that before the defendant becomes aware of the filing of a lawsuit (i.e., before a statement of claim from the court is sent to it for comments), the court may take a number of procedural steps from the filing of the lawsuit, which is the point at which the limitation period is suspended, for instance, it may take a decision on the jurisdiction of the court to rule on action, a decision on the exemption from court fees, a decision on the bias of the judge, an invitation to the plaintiff to complete the action in case of missing essential elements, etc. The defendant usually has no information about these court actions and repeated practice shows that the action comes to the attention of the bank only after a long delay. For this reason, banks can use a reasonable reserve time of two years.

5. Conditions governing the retention of personal data

Banks have obligations to ensure that information relating to the purpose of processing, categories of personal data, categories of data subjects, categories of recipients and 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 taken 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/her personal data erased and not further processed, where the legal title for their processing no longer exists.

In addition, technical and organizational measures shall be established to prevent their unauthorized processing; this should in particular include 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 personal data after the processing has been completed, 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 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 a case, it is necessary to keep in mind the rights of the clients to protection from any unauthorized interference in private and personal life and to erase personal data, or possibly to pseudonymize them as soon as possible, i.e. not process them in a form that allows the identification of the data subject.

CUSTOMER RELATIONSHIP

1. Ensuring the rights of bank 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[7],
- The processing is unlawful or no longer needed to achieve the purpose but the data subject requests them to be kept instead of erasing them[8,]
- The data subject raised an objection to the processing of personal data based on the legitimate interest of the controller or of another person[9.]

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

[7] Article 18 (1) point a) GDPR.
[8] Article 18 (1) points b) and c) GDPR.
[9] Article 18 (1) point d) GDPR.

selected data to another processing system, making the selected personal data unavailable to users, or temporarily removing the data from publicly available websites.[10]

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.

The bank may require the customer who submits a complaint regarding the restriction of the processing of personal data to provide at least a basic justification for the complaint. Banks may require that the complaint be specific and comprehensible and that the data subject concerned be sufficiently identified.

The complaint contesting data accuracy must contain a specification of the data or the category of data processed by the bank 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. The bank will proceed to restrict the processing only in this case (and inform also the data recipients) and it will initiate a review of the complaint.

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 as being inaccurate (the client, for example, objects that his/her contact address is inaccurate and the bank does not send any communication to such an address for the period of restricted processing; other personal data may, however, 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 (service as such or a service with certain parameters) in accordance with a special legal regulation. An example of the best practice is a procedure whereby 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 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 [11].

1.2 Right to erasure

The conditions under which the controller is required to erase a person's personal data[12], 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:

[10] List included in Article 67 GDPR.
[11] Article 18 (2) GDPR.
[12] The purpose of the related provisions of GDPR can be achieved both by full erasure of personal data and by their irreversible anonymization.

- Retention or other processing of personal data of the person concerned is unlawful[13],
- A legal obligation has been imposed on the controller to erase personal data[14],
- The person concerned withdraws consent to personal data processing and the controller has no other legal title for their processing[15],
- Application of the opt-out principle applied to data processing for direct marketing[16].

In the first two cases, no specifics in banks' activity are found. 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.

In a banking environment, only a very small part of the processing of personal data is performed on the basis of the consent of the persons concerned. In the case of 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 to store his/her data and the data relating to transactions with him/her even for many years after the termination of the business relationship. In the case of employees, the bank is under an obligation to manage personnel security as part of its prudential business rules, but in relation to certain groups of employees, the obligation is imposed on it by a special law (the ZSÚ, the Insurance and Reinsurance Distribution Act and in the case of certain banks, by the Act on Cyber Security). Also, the obligation to process and store a range of data on employees based on special laws, or to protect their or its legitimate interests, is imposed on the bank as an employer.

As for 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 communication sent to electronic contacts (e-mail, telephone number), because they have a separate legal regime (see Article 95 GDPR, which refers to the ePrivacy Directive, which is transposed in this part by Act No. 480/2004 Coll., on certain information society services, as amended). 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 is obliged 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 was expressed with the direct marketing. The exception contained in Article 17 (3) (b) of the GDPR shall be applied to this situation. In fact, in this instance, it is in particular a case of an expression of a 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.[17]

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 bank product, or its employees, but whose data were collected and processed by the bank especially for marketing purposes.

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:

---

[13] Article 17 (1) points a), c) and d) GDPR.
[14] Article 17 (1) point e) GDPR.
[15] Article 17 (1) points b) and f) in combination with Article 8 (1) GDPR.
[16] Article 17 (1) point c) in combination with Article 21 (2) GDPR.
17 The processing of personal data for marketing purposes is comprehensively dealt with in Chapter 2.

- ✓ 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?

When addressing this issue, it is necessary to rely primarily on the meaning of the right to erasure, which is usually an irreversible destruction of other than identification data (direct identifiers), in particular data relating purely to personal, economic, social or cultural identity. On the other hand, the mere storage of the identification data of the subject for an adequate period, not their active use, together with information on the categories of personal data processed by the controller, in what period and for what purpose the controller processed them and information on the realization of the erasure, in particular in the form of a log, and the related communication with the data subject, can be described as data processing which is necessary to protect the legitimate interest of the controller[18]. This interest is the ability to prove the fulfilment of the request made by data subject and thereby fulfilment of Article 17 GDPR and the controller thus avoids the risk of sanction[19], or of 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 above-mentioned scope 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 in their storage persists, as none of the cases provided for in Article 17 (1) of the GDPR relate to them.

According to legal regulation, a procedure can also be considered as acceptable, where an irreversible erasure of all personal data, or an irreversible erasure of the data subject's identification data is performed, and the remaining personal data become anonymized 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 in this case for the controller to be able to prove that it has established rules for the liquidation of all personal data or identification data, according to pre-defined periods, and that it does not keep the data any longer (all personal data have been irrevocably erased) or that it otherwise does not process any remaining personal data, for which the prescribed period of their processing has already expired, or for which it does not have the title to process them.

Both options are possible. It will always depend on the specific bank, the data controller, which one it will choose, 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 the actively used databases and systems. The obligation to immediately erase the data does not have to be applied to the same extent also in systems intended solely for storing the data; in their case 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 where 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 a

18 At least for the duration of the limitation or prescription period.

19 In accordance with Article 83(5)(b) of the GDPR, a fine of up to €20,000,000 or 4% of the Group's total worldwide annual turnover for the preceding financial year may be imposed for breach of the obligations laid down in Article 17 of the GDPR.

particular client and proceeds to shredding only after the expiration of the statutory period after the expiry of the last of the similar products provided to that client.

1.3 The right to portability

Portability means a transfer of certain data of the data subject from one service provider to another or to the data subject itself. It can be said that the right to portability complements the already established right of access to personal data.

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

a) The processing is based on a consent or on a contract[20], and
b) The processing is carried out by automated means[21].

The form of transferred data

The transferred personal data should, in accordance with the GDPR, 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 without reservations, since the GDPR sets no obligation for the controller to process such data any 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 sent to the new controller. It is up to the bank to take into account and decide on the way the data is transferred and assess whether the transfer is technically feasible and safe. The fact that the bank chooses safe and at the same time reasonable means of communication, although different from that 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. The data subject is informed about this.

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 the specific request made by the data subject. The scope of the data should be limited only to the data of the data subject, given that the data subject has the right to freely dispose of his or her own personal data. Personal data that are transferred should be those 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 a consent. The right should not be applied to data that the bank derives from the behavior of the data subject. Such data may, 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 to an unlimited extent at the client's request, especially with regard to the scope of data processed by banks. An interpretation of the right to portability, which is too broad, would, moreover, be contrary to the purposes of the processing, as each controller can process only the necessary scope of data, which is why it is

[20] Article 20 (1) point a) GDPR.
[21] Article 20 (1) point b) GDPR.

not appropriate, also for this reason, for banks to provide data on payment transactions to telephone operators, for example. Moreover, when transferring data, it is always necessary to ensure that the rights of third parties are not adversely affected, the obligation to ensure the security of the data transferred is observed and that at the same time, the data subject is thus protected.

Considering the scope of data processed, the banking sector must be used as a benchmark for data security, especially for providing for a very strong data security, technically and organizationally. 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. Within the financial sector, banks will only provide information 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 extending 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 was transferred from a third party. As the banking environment places great emphasis on the security of internal systems working with data, any transfer via a media from a third-party can pose a risk threatening the banking environment with a virus or other malware. In particular, the right to portability should be fulfilled when using the 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. mobility in the banking environment

A special regulation of portability in the field of payment accounts exists in the banking environment based on the Payment Services Directive, which is transposed in the Czech Republic by Act No. 370/2017, Coll., the Payment System Act (hereinafter referred to as the "ZPS")[22]. In this regard, the ZPS represents a special regulation which is accorded priority application vis-a-vis the GDPR when a request for data transfer is made to another provider of the same service.

Where the rules for transferring the payment account (rules according to the GDPR vs. rules according to the ZPS) were set differently, they would be in conflict with the rules for switching 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 institute, i.e., facilitating the sectoral mobility.

1.4 The 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 to learn what a particular controller is processing with regard to the data subject. The data subject learns how the data is handled, which data the bank, as the controller or processor, processes, to whom the data can be provided, and from where it is obtained. This right is only activated after the data subject lodges his/her request.

22 Compare Sections 203 – 209 ZPS.

Form of information provided to the data subject

In accordance with Article 12 of the GDPR, it is necessary 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 sort the information from the systems and provide it so that the data subject understands the data. Information may be provided to the data subject both orally (if the data subject requires) and in writing (physically on paper/electronically). Information provided electronically can be provided in the commonly used electronic format (for instance pdf, xls, csv, etc.); it is at the discretion of the bank to decide whether or not to choose such a format.

Methods of transferring information

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

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., which 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 to other subjects-recipients and other 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 what 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 and layering 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 since 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 are at his/her disposal, such as, for example, transaction data available in internet banking or provided in the account statement. The controller always informs the data subject of the purposes of the processing and of the data categories being processed as well as of other prerequisites of processing; this, however, can be done on a general level with reference to the individual categories of data.

The individual stages of executing the request:

a) Identification of the client

When 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 based on verifying 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, a verified 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, but the data subject should, at the same time, have an opportunity to choose the identification that represents the least obstacle for the data subject from more than one possible forms of identification.

b) Confirmation of personal data processing

The bank has a duty to disclose whether or not it processes his/her personal data to the data subject. After such confirmation, the bank is obliged to provide specific information on the processing without any undue delay, usually within one month of lodging the request and in justified cases within 3 months at the latest. A reasoned case may be, 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, provided of course, that both actions occur without undue delay.

Possible action by banks in 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 data that are available to the controller to the data subject. The aim is to provide a comprehensive information on 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 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 alone will 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 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, this may be the historical data (for example, the data subject may request information on payment cards issued for the entire duration of the contractual relationship).

Limits of the right of access to personal data

The right of access to personal data may be limited just as every other right has its limits. 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[23]. The disproportionate effort could, for example, be the provision of technical data on backup tapes which are no longer used for carrying out active operations, or it could be information where 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 (typically, these could be prudential requirements arising from the ZOB, AML, the Criminal Procedure Code, the Code of Civil Procedure, etc.).

Whereas the GDPR considers not only an active activity related to data but also their storage as processing, which means inactive processing, where the controller does not actively use personal data for its activity any more (fulfilment of the contract), the law requires the controller to store personal data in the sense of temporary archiving (typically, it may be personal data stored with the controller on different repositories, such as backups, archives, tapes which are not actively used by the controller); it

[23] Compare recital Article 62 GDPR.

is necessary to determine what level of detail will be provided to the data subject. Indeed, if it would in practice mean that the data subject would be provided with all the information that the controller does not use actively, other than to comply with legal obligations to store data, the controller would have to use disproportionate efforts to "revive" the historical data. Therefore, as long as the data subject does not reasonably require specific historical data, it is considered sufficient to provide the data subject with actively used personal data.

2. Marketing

2.1 Direct Marketing

Banks use different ways to reach out to their clients in their business activities. 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 the legitimate interest in accordance with Article 6, Section 1, point f) of the GDPR. However, the GDPR 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 such marketing.

a) Legitimate interest in direct marketing

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* notifications, and mail. In order to ensure the rights of the addressees, an objection may be raised against the legitimate interest in direct marketing in the case of individual banks. Banks may use personal data for the purposes of direct marketing, if there is a connection between the purpose of the processing of data and the bank's offer.

It is not possible to raise objections against the 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. This 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) Expectedness of marketing offers on the part of clients

All banks are business entities that seek 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 requesting his/her prior consent. Products of other businesses that are members of the group can also be offered by the bank itself, such as savings, insurance, investing, etc., or other payment services, while they must comply with the transparency requirements in accordance with Article 5 of the GDPR, i.e., in particular, provide a list of members of the group. Banks may use legitimate interest within the meaning of the GDPR to reach clients, but they can also reach clients in accordance with Section 7 (3) of Act No. 480/2004, Coll. Banks must comply with the appropriate method of informing of the reason for sending such offers and the method of unsubscribing from them. For more details, please see Point 2.5.

2.2 Categorization and profiling in direct marketing

a) Simple categorization – legitimate interest

In the interest of objectivity, banks work with several types of categorizations 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. During the processing, data subjects - clients are organized into certain target groups (chosen, for example, according to their specific place of residence, specific product, etc.). The client may also receive a product offer that is offered within a particular financial group as part of this offer.

b) Advanced categorization, or gross segmentation - legitimate interest

Banks use advanced 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 adequate service, for instance, receiving corresponding marketing offers in accordance with selected data. Within this categorization, an offer from another specific financial group entity can also be sent to the client, if the subject of the offer is an expected service, i.e., a service complementing or extending products, which the client has already concluded with the bank.

c) Profiling in marketing – consent

Banks process a large amount of personal data of individual clients in their activities. Typically, this may include processing different combinations of data and indicators about the client to create a profile with his/her preferences and anticipated needs. This kind of processing serves to better understand the client's behavior and consequently to keep this information permanently above a particular client, rather than being a specific individual targeting. Advanced statistical and analytical methods are used in the processing, including, for example, artificial intelligence technologies. The processing of the client's personal data in this manner already requires consent from the client, both for the creation of the profile itself and for its subsequent use in marketing.

2.3 Pre-approved credit limits

The provision of credit products represents one of the key activities of banks. An offer of a pre-approved credit limit 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 customer service. In this case, it is not a marketing activity in the true sense of the word until the moment when a targeted communication of the pre-approved limit is sent to the client, or of information derived from it.

2.4 Existing customers satisfaction surveys

Banks seek to provide quality services to their customers and to 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 centers, 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 in ascertaining interest of specific products, etc. If the communication has a form of a commercial message, it is necessary to comply with the conditions stipulated by Act No. 480/2004, Coll.

2.5 Commercial message vs. service and technical messages

Further to the legislation mentioned above, banks must also apply other legislation, for instance, Act No. 480/2004 Coll., on Certain Information Society Services, as amended, where it comes to certain forms of marketing messages (for instance e-mail, SMS). The controller may disseminate commercial messages 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 messages. In addition, such commercial message is properly identified by the words 'commercial message or by 'CM', while the identity of the sender may not be concealed. A valid address must also be available in such a commercial message to which information can be sent, notifying that the addressee does not wish to receive any further commercial messages, or another way must be indicated to unsubscribe from receiving other commercial messages. In the case of banks, such a commercial message may be, for example, 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. Information sent to clients about the success of the bank or its products in competitions to promote the bank's brand or product sales is also a commercial message.

Nevertheless, banks can communicate with their clients not only via marketing communication or by sending commercial messages, but in selected cases, they must inform their clients for instance, about legal documents (change in product conditions, bank account statement, annual statement of fees, 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 error. Similarly, the client may be informed that a bank branch is closed due to a technical failure or reconstruction, about changes in the opening hours of the branch, etc.

In such cases, this is not a commercial message 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.

However, if a service message is combined with a message that is a commercial communication, the rules for commercial communications apply.

2.6 Cookies

Financial institutions use cookies when operating websites. Banks that use cookies provide web users with explanatory information and the option to set cookies, based on the opt-in principle. This information must be available on every website or sub-site of the bank, including internet banking, mobile and desktop applications.

Minimum information that banks publish on their websites contains:

- A basic explanation of what cookies are,
- An explanation of the purpose of cookies and their benefits to users,
- Types of cookies in the basic categories (e.g., Necessary/Technical, Functional/Preferential, Statistical and Marketing) and an explanation of these,

- A list of cookies used on the website (differentiating at least 1st and 3rd party cookies), the retention period, the specification of information stored in them, a description of their functionality and the legal title applied to their processing (e.g., legitimate interest or consent),
- Instructions on how to change the settings of cookies or how to delete them.

3. Information obligation

The data subject has the right to be provided with information defined in Articles 12-14 of the GDPR.

While providing this information, the principles of transparent communication, a comprehensible form of language and legibility have to be taken into account in particular. Therefore, it is appropriate to layer the volume of provided information while providing for maximum transparency. The bank will at least provide basic information in accordance with Article 13 (1) of the GDPR, or Article 14 (1), GDPR as the first level information. More detailed and supplementary information (in particular in accordance with Article 13 (2) of the GDPR) may be provided by providing a link, or on another page. In the on-line environment, a gradual instruction regarding 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).

Banks generally fulfil their information obligation by publishing the Information on the processing of personal data ("Information Memorandum") on their websites. The Information Memorandum must be clear and comprehensible (it must in particular avoid the use of highly technical terms, legal formulations), complete within the scope of the requirements of Articles 13 and 14 GDPR, and easily accessible. It is good practice to create a privacy section on the website that can be accessed directly from the homepage. The Information Memorandum containing all routine processing carried out by the bank may be supplemented by sub-Information on specific or temporary processing (for instance, in connection with the implementation of emergency government measures, etc.).

Banks shall provide information pursuant to Article 13 of the GDPR at the time when they obtain personal data from the data subject. It is good practice to provide this information by means of an Information Memorandum, which is available to the data subject during the meeting (on paper or in electronic form) and can be physically taken away or received electronically (for instance, to his/her email address). A link to the published Information Memorandum is included in the documents conveyed to the client. It is advisable to provide clients with selected specific information about the processing in addition to the link to the general Information Memorandum, particularly in the on-line environment.

Acquainting the client with the above at the beginning of the meeting is sufficient. If the controller obtains additional data, or for other purposes not already communicated, it shall inform about them by updating the Information Memorandum on the website. Clients are notified of material changes to the Information Memorandum. Information does not need to be provided to the data subject if the data subject has the information.

If personal data is not obtained directly from the data subject, i.e., where the controller takes over data from another entity or controller, the information obligation may be transferred to the other person in justified cases, in particular where unreasonable efforts would be required to convey the information (for example, the client's obligation to inform an insured person other than the policyholder).

The information obligation does not apply to processing on the basis of a legal obligation, in public interest (for instance, security), or on the basis of special laws - FATCA, AML, fraud prevention, or if the purpose of the processing of personal data would be threatened. At the same time, other rules are laid down to protect the 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 customers-legal entities. The application of the GDPR thus 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 contact details, if they do not contain personal data of natural persons (telephone exchange, e-mail address in the form „info@firm.cz“,etc.).

However, as soon as personal data relating directly to specific natural persons are processed when legal entities are serviced, or as part of fulfilment of contracts concluded with the bank's suppliers, the provisions of the GDPR have to be applied to the processing as appropriate. Processing of the address of permanent residence, private telephone number, number or copy of the identification document, date of birth or birth number of the person can serve as an example of this procedure. In such cases, the appropriate legal title 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 title and purpose of further processing.

In this situation, this relates most frequently to data on specific natural persons authorized to represent the client, whether data of members of statutory bodies of the given corporations, persons authorized to use accounts or to communicate otherwise in relation to the fulfilment of the agreed product or service, or use payment cards. In these cases, it is necessary to process the personal data of those persons, in particular for the purpose of their proper identification.

In this respect, the bank must therefore adequately comply with the requirements of the GDPR to minimize in particular the amount of data processed, to determine the periods of their processing, and to provide for updating the data accordingly.

Compliance with information requirements can be very impractical or even impossible in these cases. The bank should therefore inform the data subjects concerned of processing their data directly only if this 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 person in the form of data of its employees), the legal person itself which transfers the data to the bank should accordingly inform the natural person about the data transfer (for example, this may be the transfer of data for the purpose of issuing, transferring and using business credit cards). At the same time, the inclusion of this procedure in a contract between the bank and the legal person may be considered. The obligation to appropriately update data of natural persons may be regulated in the same manner.

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 of the ultimate owners of legal entities processed for the purposes of the AML Act, or storage of data on executed transactions for the purposes of the fulfillment of the ZoB, can be performed on the basis of the legal title of fulfillment of legal obligation. Such processing therefore does not need to be further specified and the data subjects of this processing need not be informed.

In relation to clients of legal entities, there are a number of cases where these clients request that the transfer of personal data of their employees carried out by means of a regular payment system (for example, payment of wages, reimbursement of business trips, etc.) be part of the processing contract concluded with the bank, in which the bank would be in the role of processor. In this respect, however, it is true that banks, while providing their product, comply with the instructions given by the client, i.e., they perform the transactions in question, but are not in the role of the processor, which would perform the processing of personal data on behalf of the operator (client), taking into account the specific legal provisions for the provision of the product (ZPS, ZoB). There is therefore no need to conclude a specific contract or amendment to the processing of personal data in these cases, beyond the existing contractual relationships.

5. Automated individual decision making, including profiling

New fully automated procedures for a more efficient provision of financial services and proper compliance with regulatory obligations are being developed and implemented in connection with the need to process large amounts of personal data when providing banking services. 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, and to reduce the likelihood of human error or prevent fraudulent behavior.

In the customer service itself and in 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 benefits the client in the first place. For example, in a fully automated process, the system can decide on an application for a loan (in particular a consumer loan), including the setting up of the applicant's risk profile, or, for instance, or setting up the investment profile, when concluding investment products or a mortgage credit, or detect fraudulent behavior without human intervention in the environment of electronic channels, etc.

The input for the automated decision may be personal data provided directly by the data subject (for instance, identification and contact details) or 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 made with the use of 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[24] do not apply to decision-making which is based only on a 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.

[24] Particularly Article 22 GDPR.

For example, if a loan application is processed and evaluated automatically, but the decision to grant the loan is the responsibility of a person appointed by the bank's internal rules and procedures, who, after taking into account all factors of the application, has the ability and obligation to take a decision which is different from the automatic assessment (recommendation), it is not an automated decision.

The appropriate legal title for automated decision-making (including profiling) is the following:

- Consent of the client,
- Conclusion or performance of a contract to which the data subject (client of the bank) is a 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 make an assessment of whether the data subject should not be informed when personal data are entered in the process itself (for instance, information that the process is an automated decision-making is clearly indicated in the loan application form that the client fills in the electronic channels 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 (natural person, data subject) has the right not to be a subject to a decision which is based solely on an automated processing, including profiling, which produces legal effects impacting him or her or affects him or her significantly in a similar manner. 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 an 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 the need to maintain a consistent and transparent approach to all data subjects and to ensure the speed and efficiency of the appropriate

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.

Given that automated decision-making is based on a systematic and extensive evaluation of the personal aspects relating to natural persons, which is based on automated processing, including profiling, and on which decisions are based that produce legal effects on natural persons or significantly affect the natural person in a similar way, the controller, when preparing such processing or when preparing a new process, has a duty, to

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

It is fully under the responsibility of each controller to select the tools and procedures that it will use to process personal data. When implementing a process of automated processing (and then throughout the existence of the process), the controller must, however, 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 ensuring the privacy of the data subject by less invasive procedures/methods, i.e., that the automated decision-making is an adequate 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 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.

SPECIFIC RULES FOR PROCESING PERSONAL DATA OF BANK EMPLOYEES

In order to provide for the stability of the bank and with a view to the interconnectedness of the banking sector and therefore also the stability of this sector of 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 to implement an adequate internal control system.

Detailed requirements for risk management, the bank's management and the 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' security 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 its 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 on 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 a vacancy and in the course of the employment relationship. For certain job positions, a thorough assessment of the integrity of the applicant is directly imposed by a special legal regulation [25], 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 the privacy of the persons concerned.

Among the facts that have to be usually assessed when reviewing the level of risk of a job, respectively when performing the proportionality test, there 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, directly or indirectly, unauthorized manipulation with the assets of the bank or of its clients,
- The quality and functionality of automatically performed checks of the employee's activity and
- 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 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 the employee or the 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 the job applicant, and have sufficient legal grounds to do so, 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 Labor Code.

RELATIONSHIP WITH THE SUPERVISORY AUTHORITY

Data breaches

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

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, like certain other regulations[26], requires banks to notify certain types of security incidents to the supervisory authority, the UOOU, (taking into regard the exception in accordance with Section 12 of Act No. 110/2019, Coll.), and in certain cases directly to the persons concerned.

- ✓ In order to assess whether a particular security incident corresponds to the definition of a personal data breach in accordance with the GDPR[27], account should be taken of whether it related to personal data processed by the bank, be it data of clients, employees or of 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 personal data being processed, but only a real incident resulting in the above-mentioned consequences, i.e., in interference with confidentiality, integrity or availability of personal data. Therefore, a situation where a security error was identified that could only potentially lead to an unlawful disclosure of data would not be a security breach. A breach would happen where, for example, a genuine abuse of a weakly protected employee's mobile phone occurred, which would result in the above consequences.

Where personal data have been transferred to a person other than the authorized addressee (for instance when sending an account statement) it is decisive whether it can be demonstrated that the wrong address was communicated to the bank by the authorized addressee (e.g., the addressee did not update the mailing address or telephone number). In such a case, there is no breach of security.

- ✓ 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 who should assess whether or not to escalate the incident further.

It is therefore possible to conclude that the nomination 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 the 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 that a breach of personal data occurred with a high degree of probability. 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

[26] ZPS, the Act on Cyber Security.
27 Article 4 (12) of the GDPR

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 the notification is made within a given deadline, or later. By analogy, the start of the time limit for reporting to the UOOU can also be concluded for breaches identified by the processor entrusted with processing by the bank, i.e., from the moment when the processor had or should have had sufficient information to establish that a personal data breach was likely to have occurred with a high degree of probability.

The bank follows a similar procedure where it has a duty to notify the affected data subjects of the incident, which must be done without undue delay.

✓ Assessment of the 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, depending on 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 and shall be 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[28]. However, the assessment must always be individual, not mechanical, taking into regard the context and the probable impacts of the given case.

PERSONAL DATA SHARING

1. Client registers

Banks share the necessary personal data with respect to natural persons, loan applicants among themselves in order to verify the financial standing and creditworthiness of the loan applicant. Sharing

[28] ENISA recommendations are an appropriate standard, available at https://www.enisa.europa.eu/topics/data-protection/personal-data-breaches

can also take place with other non-bank entities which pursue the same purpose (verification of the trustworthiness and payment discipline of applicants for a service). The sharing of personal data for the purpose described above is performed via so-called client registers, which banks may use.

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

BRKI – Client Information Bank Register

The legal title for the processing of personal data and information on all relevant banking products obtained by the bank from the BRKI register is the fulfilment of the legal obligation of the bank - the controller - based primarily on the requirements of the ZoB and the ZSU.

NRKI – Non-Banking Register of Client Information

The legal title for the processing of personal data obtained by the bank from the NRKI register is the fulfilment of the legal obligation of the user of the register - the bank - the controller - arising in particular from the Consumer Credit Act, but also from other regulations governing the obligation to verify the creditworthiness of the applicant for a financial product and to prevent his/her over-indebtedness.

The processing of personal data related to the granting of other than consumer credit to natural persons is based on the legitimate interest of the users of the register.

Data sharing between the BRKI and the NRKI registers

From the perspective of banks, the legal title is the fulfilment of the legal obligation of the data controller, based primarily on the ze ZoB and the ZSÚ.

b) Registers Solus

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

The legal title for the processing of personal data obtained by the bank from negative registers SOLUS is in the legitimate interest of the bank – the controller – in accordance with the Consumer Protection Act. [29]

Positive register Solus

The legal title for the processing of personal data obtained by the bank from the positive register Solus is the consent of the data subject in accordance with the Consumer Protection Act.[30]

Detailed rules are provided in documents through which individual registers of clients fulfil their information duty. An example of good practice is a procedure whereby banks inform their clients and

29 Section 20 (1) of the Consumer Protection Act.
30 Section 20 (6) of the Consumer Protection Act.

applicants for credit products about the processing of their data in client registers at least in a general manner (for instance in the form of an information memorandum) and refer to disclosure documents of the relevant registers for details.

2. Cooperation in the field of 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 the 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 him/her in order to fulfil his/her statutory obligation resulting, in particular, from the regulation of the distribution of financial products,

b) If he/she is authorized to process them for his/her own purposes if the client has given consent (for instance, for marketing purposes),

c) If he/she is obliged to process them for the purpose of performance of the contract with the client,

d) If he/she processes them based on his/her 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 he/she 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 him/her as consumer credit intermediary from the ZSÚ), is in position of personal data controller.

In certain cases, even both subjects who are part of 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 authorized 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. The transfer of data in this case requires the explicit and express (i.e., identifying the specific bank or banks or other controllers to which the data may be transferred) consent of the interested party, which the intermediary is responsible for obtaining and documenting.

In the case of so-called additional services to the bank's products, such as, for instance, payment card assistance services, the bank and the service provider may be in a relationship of joint controllers to the extent of processing the customer's data proving entitlement to the service. If the service provider itself provides the service under its own name and responsibility, it is a separate controller of the service user's data in this part of the process.

The contractual treatment of the processing of personal data should then also correspond to the specific type of mutual cooperation. In addition to the usual data processing contract between the controller and the processor under the GDPR, a data processing contract between two controllers or joint controllers, or a combination of both types of contracts, may also be appropriate in some cases.

3. Data sharing within a financial group (consolidated entity)

   Banks may only share personal data with third parties within their financial group (i.e., with parent, sister or subsidiary entities, including in other countries) if they have one of the legal titles under GDPR Article 6 to do so. The general principles for the transfer of personal data within a group of undertakings to an undertaking located in a third country remain unaffected.

   Recital to Section 48 of the GDPR states that controllers may have a legitimate interest in the transfer of personal data within a group of undertakings for internal administrative purposes, including the processing of personal data of customers or employees.

   At the same time, banks must respect the requirement to protect banking secrecy. The conditions under which banks may share data are set out in the Act on Banks (ZoB). In particular, according to Section 38b, banks may transfer data for the purpose of complying with prudential rules. Such purposes include, for example, credit or other risk management, fraud prevention, etc. The sharing of data to the extent necessary for these purposes can thus be considered a legitimate interest under the GDPR.

   Data sharing for marketing purposes is generally based on the consent of clients.

4. Banking Identity

As of 1 January 2021, banks and branches of foreign banks are authorized to provide identification services within the meaning of Section 1(4)(c) of the ZoB and thus act as identity providers (IdPs). As of 1 January 2021, it is therefore possible to provide electronic banking identity (EBI) and related services to various online service providers (SePs).

Where banks provide EBI services, the following are involved as separate personal data controllers:

a) Banks in their role as IdPs, confirming the identity of bank customers and SeP customers (hereinafter referred to as 'customers' or individually as 'customer') on the basis of the identification of the customer in the IdP interface via the EBI;
b) On-line service providers as SePs, to which the customer proves his/her identity using EBI; and
c) An identification service provider pursuant to Section 38aa of the ZoB, which, on the instruction of the data subject transfers the personal data necessary to identify the customer from the IdP to the selected SeP; the identification service provider pursuant to Section 38aa of the ZoB in the EBI system is currently Bankovní identita, a.s., ID No.: 095 13 817, with registered office at Smrčkova 2485/4, Libeň, 180 00 Prague 8 (hereinafter the "BankID").

EBI and related services may be provided by banks in the position of IdP in two regimes, namely:

a) Through a qualified electronic identification system pursuant to Section 2 of Act No. 250/2017, Coll., on Electronic Identification (hereinafter referred to as "ZoEI");
b) Outside the qualified electronic identification system pursuant to Section 38 ab (1) of the ZoB.

Banks provide EBI within the framework of the qualified electronic identification system through the National Identification and Authentication Point within the meaning of Section 20 of the ZoEI (hereinafter referred to as "NIA"). EBI is available within the NIA to public SePs, i.e., state authorities and local self-government units. This mode of use of the EBI thus allows it to be used, for example, for client access to the Citizen Portal (portal.gov.cz), the portal of the Czech Social Security Administration and other eGovernment portals. Some banks have allowed their clients to use EBI in this regime as of 1 January 2021. BankID is not involved in any way in the provision of EBI and related services in this mode and EBI services are provided by banks directly through the NIA.

Outside the framework of the qualified scheme, banks can then provide identification services on a contractual basis to private SePs such as telephone operators, energy providers, insurance companies and other commercial entities. To this end, banks may provide their services to SePs either directly or through an identification service provider as defined in Section 38aa of the ZoB.

EBI services consist of confirming the identity of natural persons and providing selected data on natural persons by IdPs (banks) to SePs. In this respect, EBI services are always provided in relation to a specific bank customer upon the customer's instruction and with the customer's consent in relation to banking secrecy under the Act on Banks. Consent in this case is given for the transfer of the client's personal data from IdP to SeP.

The provision of the EBI service is thus always initiated by the customer who indicates that he/she wants to use the BankID service for his/her identification by selecting it in the environment of the specific SeP. Subsequently, he/she chooses which specific IdP (specific bank) he/she wants to use for the identification in the BankID environment. In the bank's environment, he/she confirms the scope of the data to be transmitted to the SeP and these data are transferred from the IdP (bank) to the SeP by BankID.

The legal basis for processing in the context of the provision of EBI services on the part of banks is the performance of a contract with the customer within the meaning of Article 6(1)(b) of the GDPR, namely a contract under which the services and products of the bank are provided to the customer and which also includes the issuance of electronic means of identification and the provision of identification services. Personal data processed on the basis of the performance of a contract will generally be retained by the banks for the duration of the relevant contract, unless further processing based on another legal title requires further retention (for example, for compliance with legal obligations).

The legal basis for processing on the part of BankID is the legitimate interest of the controller within the meaning of Article 6(1)(f) GDPR, consisting of:

a) The provision of identification services so that BankID can fulfil its integration role in the EBI system and ensure the provision of EBI services and the transfer of client data from the IdP to the SeP;
b) Protection of the legal claims so that BankID is able to conduct a possible future defense of legal claims brought against BankID by a SeP or by third parties.

The processing can be based on the legitimate interest of BankID, as BankID stores personal data for a very short period of time and then pseudonymizes them, so the processing does not have a significant negative impact on the interest of clients as data subjects. On the contrary, processing in connection with the provision of the EBI service provides the client with reasonable assurances that there will be no unauthorized access to the SeP user account (including unauthorized access to personal data stored in the SeP service) by another person pretending to be the client in relation to the SeP. Also, the processing of personal data is in the interest of all stakeholders, i.e., BankID, IdPs, SePs and clients, as well as in the interest of the entire market ecosystem, as the use of BankID enables to interconnect all participating IdPs and SePs and thus an efficient provision of EBI services across the market of the scale intended by the legislator.

In the context of the transfer of IdP provision data to a specific SeP, BankID processes the data to the extent required by the EBI service only for the time technically necessary to carry out the transfer. Subsequently, only the pseudonymized data of the specific IdP transaction are retained for the purpose of proving the provision of the specific identification service. In relation to the purpose of protecting BankID legal claims, the processing period will be determined by the duration of the limitation period (i.e., 15 years).

The legal basis for processing on the part of SeP will always depend on the specific relationship between SeP and the client and the purpose for which the client initiates the EBI service vis-à-vis SeP. In practice, this may be the performance of a contract (e.g., to verify the identity of the client before entering into a contract with SeP), the performance of a legal obligation (e.g., to identify the client within the meaning of Section 7 of the AML Act) or the legitimate interest of the controller.