CIB BANK

Policy V – 114

Data Protection and Data Security Policy of CIB Group

A CIB Csoport Adatvédelmi és adatbiztonsági Szabályzata

Chapter I.

Date of coming into effect: 25 May 2018

Table of contents

Chapter I: Data Protection Policy of CIB Group

1. General section

1.1. Purpose of this chapter of the Policy

The purpose of this chapter (hereinafter: Chapter I) of the Data Protection and Data Security Policy (hereinafter: Policy) is to ensure that the data of the customers of CIB Bank Zrt. (hereinafter: Bank) and other members of the group of companies operating with the Bank's participation whose main establishment is in Hungary (hereinafter together with the Bank: Controller), as well as of any other natural persons entering into a relationship with them, is processed within legal parameters, in compliance with the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council (hereinafter: Regulation) and Act CXII of 2011 on Informational Self-Determination and Freedom of Information (hereinafter: Information Act).

1.2. Organisational scope of this chapter of the Policy

The effect of this chapter of the Policy shall extend to the Bank, to other members of the group of companies operating with the Bank's participation whose main establishment is in Hungary, and to any such persons whose data is included in the data processing procedures falling under the effect of this chapter, as well as to those persons whose rights or legitimate interests are affected by the data processing.

1.3. Material and territorial scope of this chapter of the Policy

Chapter I only applies to cases of data processing performed as a financial institution.

The material scope of Chapter I extends to any case of data processing of the Controllers that:

a) includes the data of persons *who are in a customer relationship* with them,

b) includes the data of persons *who were in a customer relationship* with them,

c) includes the data of persons *who intend to enter into a customer relationship* with them,

d) includes the data of persons *who are related to their customers* in such manner as the processing of their personal data is required for providing the service,

e) is required for compliance with their legal obligation.

Territorial scope of this chapter of the Policy extends

a) to data processing activities conducted solely in Hungary,

b) cross-border data processing conducted by the Bank or other members of the group of companies operating with the Bank's participation whose main establishment is in Hungary, as exclusive controllers, and

c) data processing activities where the main establishment is Hungary.

However, the effect of this chapter of the Policy shall not extend to the data processing of the group of companies operating with the Bank's participation performed on the basis of binding corporate rules and group data processing in which the Bank participates as a controlled organisation and/or a representative.

Special cases of data processing (e.g. data processing involving installation of cookies) are subject to the provisions of special policies.

1.4. Legislative background

- REGULATION (EU) 2016/679 of the EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC,
- Act CXII of 2011 on Informational Self-Determination and Freedom of Information (Info tv./Data

Protection law),

- Act CCXXXVII of 2013 on Credit Institutions and Financial Enterprises (Hpt./Banking Act),
- Act CXXXVIII of 2007 on Investment Firms and Commodity Dealers and the Regulations Governing their Activities (Bsztv./Investment Services Act),
- Act LXXXVIII of 2014 on Insurance Activity(Bit./Insurance Act), and

any such legal regulations as contain obligatorily applicable data processing provisions.

1.5. Definitions

When applying this Policy, the following terms shall be understood in accordance with the definitions set out below.

a. **'personal data'** means any information relating to an identified or identifiable natural person (hereinafter: 'Data Subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

b. **'processing'** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

c. **„ 'restriction of processing'** means the marking of stored personal data with the aim of limiting their processing in the future;

d. **'profiling'** means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

e. **'pseudonymisation'** means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

f. **'filing system'** means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

g. **'controller'** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;; for the purposes of this Policy, the controller is the Bank and other members of the group of companies operating with the Bank's participation whose main establishment is in Hungary, and third parties in a controller relationship with them,

h. "**processor**": a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Bank or another Controller.

i. **'recipient'** means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

j. **'third party'** means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

k. **'consent'** of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

l. **‘personal data breach’** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

m.**‘genetic data’** means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

n. **‘biometric data’** means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

o. **‘data concerning health’** means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

p. **‘main establishment’**:

pa) as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment;

pb) as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation;

q. **“representative”**: a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to the provisions of the Regulation, represents the controller or processor with regard to their respective obligations under this Regulation;

r. **“enterprise”**: a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;

s. “**group of companies**”: the controlling company and the companies controlled by it; other members of the group of companies operating with the Bank’s participation whose main establishment is in Hungary: CIB Bank Zrt., CIB Lízing Zrt., CIB Biztosítási Alkusz Kft.

t. **“binding corporate rules”**: personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity;

u. “**supervisory authority”**: an independent public authority which is established by a Member State pursuant to the provisions of the Regulation; in Hungary, the Hungarian National Authority for Data Protection and Freedom of Information (hereinafter: NAIH);

x. **“supervisory authority concerned”**: a supervisory authority which is concerned by the processing of personal data because:

xa) the controller or processor is established on the territory of the Member State of that supervisory authority;

xb) data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or

xc) a complaint has been lodged with that supervisory authority;

y. **“cross-border processing of personal data”**:

ya) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or

yb) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State;

v. **"information society service":** a service as defined in paragraph (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council;

w. "**international organisation**": an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.

2. The identity and service of the Controller

The Controller is the Bank (CIB Bank Zrt., registered office: 1027 Budapest, Medve u. 4–14; company reg. no.: Cg. 01-10-041004; tax no.: 10136915-4-44), which is a credit institution falling under the effect of Act CCXXVII of 2013 on credit institutions and financial enterprises (hereinafter: Credit Institutions Act) and Act CXXXVIII of 2007 on investment firms and commodity dealers and the regulations governing their activities (hereinafter: Investment Firms Act). The Bank primarily provides its customers with the financial and investment services defined in the Credit Institutions Act and the Investment Firms Act. Beyond this, the Bank only provides the services defined in the legal regulations relating to it. The services provided by the Controller are described in detail in the Controller's general contractual documents (Business Regulations, General Contractual Conditions).

The group members listed in section 1.5 are also Controllers; they perform their data processing in accordance with this Policy and their own contractual documents (Business Regulations, General Contractual Conditions).

Where two or more controllers jointly determine the purposes and means of processing, they shall qualify as joint controllers. Joint controllers shall in a transparent manner determine their respective responsibilities for compliance with the obligations under the Regulation, in particular as regards the division of responsibilities between them in relation to their duties to provide information on the exercising of the rights of the data subject and on the data processing. The arrangement between them may designate a contact point for data subjects. The arrangement shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the Data Subjects. The essence of the arrangement shall be made available to the data subject. Irrespective of the terms of the arrangement, the data subject may exercise his or her rights in respect of and against each of the controllers.

3. Principles of data processing

The Controller shall proceed in good faith and in accordance with the requirements of integrity, in cooperation with the Data Subjects. The Bank shall exercise its rights and shall fulfil its obligations in accordance with the intended purpose of such.

The data processing must be performed in a manner which is transparent for the Data Subjects; thus, it must be clear for them how their personal data is collected, processed, used and accessed.

Personal data shall, in the course of data processing, retain its nature as such for as long as its link to the Data Subject can be established. The link to the Data Subject shall be establishable if the Controller possesses the technical conditions required for such establishment. The use of pseudonyms shall not affect the nature of the data as personal data.

In the course of data processing, the Controller shall ensure the accuracy and completeness of the data and – if necessary for the purpose of the data processing – that it is up-to-date, and that the Data Subject can only be identified for the time necessary for the purpose of the data processing.

Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the Controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the Regulation and protect the rights of data subjects.

The Controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure

that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

4. Purpose of the data processing

The Controller shall only process personal data for a specified purpose, in the interests of exercising a right or fulfilling an obligation. The data processing shall, in all its phases, comply with the purpose of the data processing. The data must be recorded and processed in a fair and lawful manner. The Controller shall ensure that only such personal data is processed that is indispensable for realising the purpose of the data processing, and that is suitable for achieving this purpose. The personal data may only be processed to the extent and for the period of time required for the realisation of such purpose.

Instances of data processing falling under the effect of this chapter of the Policy shall in all cases be related to a service provided by the Controller, which service is used or has been used by the Data Subject as a customer, or where for the purpose of using such service the Data Subject has contacted the Controller, or which service the Controller provides to a third party in collaboration with the personal involvement of the Data Subject (e.g. guarantor, the representative or the proxy of a natural-person Data Subject).

The instances of data processing falling under the effect of this chapter of the Policy may serve the following purposes:

a) preparation, conclusion and implementation of the contract with the Controller,

b) if there is specific consent for such, contact initiated by the Controller for the purposes of direct marketing or market research (by mail, telephone or by electronic or other means of communication),

c) enabling the Controller to directly assess the needs of the Data Subjects, for the purpose of providing them with higher-level services (statistics preparation),

d) risk management (analysis, evaluation, mitigation and the observance of the provisions on prudent operation, risk assumption and capital adequacy),

e) prevention, investigation and detection of abuses related to the products and services provided by the Controller,

f) compliance with the legal obligations and enforcement of the legitimate interests of the Controller, including, in particular, compliance with obligations related to the fight against money laundering and terrorist financing as well as the obligations stipulated by legal regulations governing the financial, insurance brokerage and investment services provided by the Controller,

g) allowing the Controller to assert its claims through a consistent recovery process, and to facilitate the enforcement of any settlement obligations they may have towards each other,

h) following the termination of the contract, the exercising of rights and fulfilment of obligations originating from the contract, thus in particular the enforcement of any outstanding claims based on the contract.

5. Legal basis for the data processing

The Controller shall only process personal data if the processing has a legitimate legal basis, thus:

a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

c) processing is necessary for compliance with a legal obligation to which the Controller is subject;

d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

f) processing is necessary for the purposes of the legitimate interests pursued by the Controller or by a third party, except where, according to the balancing of interest test conducted, such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

5.1. Consent of the Data Subject

If the data processing is not required for the performance of the contract, and the data may not be processed based on other legal grounds either, the Controller may only process the data if it is provided voluntarily by the Data Subject.

If the Data Subject has initiated a matter (thus, particularly, if he or she has contacted the Controller with the intention of concluding a contract), the Controller shall deem the Data Subject's consent to have been given in respect of the processing of the data provided by the Data Subject.

In the obtaining of such consent, the Controller shall always choose a solution based on which the legality of the consent can be subsequently proven. Therefore, in the case of paper-based data processing, the consent must be obtained in writing, while in the course of electronic data processing, the Controller's services involving data processing may only be usable subject to registration.

Prior to giving his or her consent, the Data Subject must be informed about all the essential circumstances concerning the processing (in particular, the identity, registered office and contact information of the controllers or processors, the scope of the data processed, the legal basis, purpose and duration of processing for each category of data, information about data transfer, advice on the legal remedies available), and must be ensured the right to withdraw such consent any time.The withdrawal of consent shall not affect the lawfulness of any processing that was conducted based on the consent prior to its withdrawal.

Where the child is below the age of 18, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.

5.2. Statutory provisions

If the processing of personal data is stipulated by a legal regulation, the data processing is compulsory. The Controller shall inform the Data Subject of this. If the legal regulation is valid and applicable, the Controller is obliged to execute it in accordance with the provisions of the legal regulation, and it may not examine the appropriateness, professionalism or constitutionality of the legal regulation.

Data processing mandatory for the Controller is stipulated mainly by the Credit Institutions Act and the Act on Insurance Services and by the legislation regulating other the services provided by the Controller (e.g. Investment Firms Act).

5.3. Performance of a contract

Personal data may be processed also where it is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract. This legal basis must be strictly interpreted, and thus it may only be applied if there is a direct and objective relationship between the data processing and the performance of the contract. The legal basis extends to data processing performed prior to the concluding of the contract and to the pre-contract relationships, provided that such processing was initiated by the Data Subject.

5.4. Legitimate interest

Data processing is legitimate also if the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

To establish the existence of a legitimate interest, a balancing-of-interest test must be conducted, as part of which careful assessment is needed, including as to whether a data subject can reasonably expect, at the time and in the context of the collection of the personal data, that processing for such purpose should take place. The interests and fundamental rights of the data subject may in particular

override the interest of the Controller if the personal data are processed in circumstances where the data subjects do not reasonably expect further processing.

Steps of the balancing-of-interest test: (i) definition of the purpose of data processing, (ii) assessment of the legality of data processing, (iii) definition and classification of the data whose processing is planned, (iv) assessment of the legal basis of data processing, (v) identification of impediments to the data processing, (vi) definition of the interest relating to the data processing, (vii) determination of the legitimacy of the controller's interests, (viii) assessment of the necessity and inevitability of the data processing, (ix) evaluation of the Bank's interest, (x) evaluation of the impact of data processing on the data subjects, (xi) any additional guarantees applied, (x) final balancing.

5.5. Protection of vital interests

Personal data may be processed also if processing is necessary in order to protect the vital interests of the data subject or of another natural person

The Controller shall inform the Data Subject about the interest to be protected that gives grounds for the data processing. The provision of information based on this section shall take place at the time that contact between the Controller and the Data Subject is established. Contact may take place subsequently, as well.

6. Scope and processing of the data

a) **Natural persons' identification data:** the purpose of processing this data is to be able to clearly identify the Data Subject and maintain contact with him or her. The Controller processes the following data of the Data Subject: name, name at birth, mother's maiden name, place and date of birth, residential address, postal address, and in the case of mandatory data processing, it also processes, as required by the law, the following data items: nationality, number of personal identity card (passport), and number of any other document that, pursuant to Act LXVI of 1992 on the registration of the personal data and address of civilians, is suitable for verifying identity.

   The legal basis for the data processing shall be the consent of the Data Subject – primarily the consent granted in the contract – and the statutory provisions.

b) **Telephone numbers and other contact information required for maintaining contact with the Data Subject:** If provided by the Data Subject, the Controller shall process his or her telephone numbers and email address required for maintaining contact.

c) **Copies and data of documents:** The Controller prepares copies of the individual data-verifying documents in order to establish the correctness of the data, based on the Data Subject's consent or a binding provision of law. If the Data Subject does not wish to give his or her consent, instead of the copy, the document presented for verification of the authenticity of the customer's data must be recorded among the customer's data, besides the fact that verification has been performed.

d) **Data stipulated by the legal regulations on the prevention of money laundering**: The Controller processes the data required by Act LIII of 2017 on the prevention and combating of money laundering and terrorist financing (hereinafter: Pmt.).

e) **Data necessary for the conclusion of the contract for the service used or intended to be used, or for making a decision on whether to conclude such a contract:** If the Data Subject wishes to conclude a contract with the Controller for a service, the Controller may, prior to contract conclusion – in accordance with the relevant contractual conditions – examine whether such contract can be concluded with the Customer or other Data Subject. If the contracting party is not the Customer, the data of the Data Subject may be processed in relation to the preparation of the contract and to the decision on whether to conclude the contract.

f) **Data generated in relation to the provision and use of the service:** The Controller processes the data generated in relation to the service provided under the contract in accordance with the stipulations set forth in the relevant contractual conditions and legal regulations (data related to invoices, receivables, account operations, transactions, etc.).

g) **Data related to rights and obligations established in relation to the provision and use of the service:** During the performance of the contract concluded between the Controller and the Customer, the parties may exercise their rights and must fulfil their obligations under the contract. The Controller may process the data related to this (e.g. data related to interest claims or breaches of contract).

h) **Data related to claims, and to the assertion of claims, arising from any existing or terminated contract between the Controller and the Customers:** According to the applicable laws, claims may arise from contracts already terminated; the Controller processes the data relating to this, which is necessary for enforcing any claims, as well as the data that must be retained based on the law.

i) **Data generated during the establishment of the contact with the Controller or with the Controller's customer service desk:** This includes all the data generated at the customer service desk during the contact between the Data Subject and the customer service desk. The data processing in this respect is strictly related to the procedure launched by the Data Subject, to the contract, and to the performance of the contract.

j) **Telephone conversation between the Customer or other Data Subject and the Controller:** The Controller records and processes, in accordance with the provisions of the applicable legal regulations and separate specific information relating to this, the voice recordings made on the conversations between the Data Subject and the customer service desk. The Data Subject is always informed about such recording prior to the start of the conversation. In matters not regulated by the law (in particular in cases not qualifying as complaint cases under the Credit Institutions Act), and in matters not required for the performance of a contract concluded with the Data Subject or for proof of consent, the phone conversations may solely be recorded on the basis of the Customer's prior informed consent.

k) **Recordings made using the voice and image recording equipment operated by the Controller:** The Controller may, at its premises, at the points of acceptance for cash-substitute payment instruments and electronic cash belonging to its own acceptance network, in its branches, as well as at any agents it may have, operate image and voice recording systems. These recordings are processed by the Controller.

l) **Data stipulated by legal regulations on FATCA**: The Bank shall handle the data stipulated by Act XIX of 2014 on the announcement of the Agreement between the Government of Hungary and the Government of the United States of America to Improve International Tax Compliance and to Implement FATCA and on the amendment of the relevant related acts (hereinafter: FATCA Act.).

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation, in absence of the legal bases specified by the Regulation (e.g. the data subject's consent, disclosure of the data by the data subject, enforcing a legal right) shall be prohibited.

7. Data processing for direct marketing and research purposes

The Controller may use the personal data of the Data Subjects, based on their consent, for the following purposes:

- Using the direct marketing method to send advertisements by electronic mail (including faxes and short text messages) or via automated tools by phone;
- Contact by electronic mail (including faxes and short text messages) or via automated tools by phone, for market research and public opinion polling purposes;
- Contact by electronic mail (including faxes and short text messages) or via automated tools by phone, for measuring customer satisfaction and developing the service.

A condition for the use of the data in accordance with the above is that the Data Subject grants his/her consent thereto. Such consent is always voluntary, and the Controller may not stipulate it as a precondition for contract conclusion. The Controller may encourage the giving of consent according to this section by offering the possibility of participation in certain prize competitions and promotions.

The Data Subject may withdraw his/her consent to the data processing referred to in this section at any time, without explanation.

The Controller shall, on the occasion of each contact, inform the Data Subject about his/her right to withdraw his/her consent, and the withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

Until the Data Subject's objection, the Controller is entitled to send, by post or via a non-automated phone call to the Data Subject's postal address or public phone number, inquiries for the above purposes, with the proviso that any advertising, in absence of consent, may only be sent in an addressed advertising message.

8. Individual cases of data processing

8.1. Recording of telephone conversations

The Controller is entitled and obliged to record telephone conversations in the cases specified by law, in particular the Credit Institutions Act and the Investment Firms Act. Moreover, the Controller may record the phone conversation on the basis of the Regulation if it is required (i) for the performance of a contract concluded with the Data Subject, or (ii) prior to the conclusion of a contract, to take the steps at the Data Subject's request, and (iii) to prove consent given by the Data Subject. In other cases, the conversation may only be recorded with consent based on prior information as specified in section 5.3. j).

The retention period of the voice recordings is (i) in the case of consent-based recording, until the consent is withdrawn, (ii) in the case of mandatory voice recording ordered by law, the statutory retention period (e.g. in the case of complaints, 5 years), (iii) in the case of performance of a Contract, until the lapse of claims arising from the legal relationship, (iv) in the case of recording consent, the duration of processing the data covered by the consent.

8.2. Preparing image and voice recordings

The Controller may, at its premises open for customers, at the points of acceptance of cash-substitute payment instruments and electronic cash belonging to its own acceptance network, at its branches and at its agents, if any, prepare photographs of the Data Subject performing a transaction or visiting such locations, and the Controller may store and use such photographs for purposes of settlement of accounts and security. The Controller keeps these records in compliance with the relevant legal regulations, for not more than 60 days.

8.3. Contacting for purposes of cross-checking data against the state records

Based on the Data Subject's consent, the Controller is entitled to *check* the data provided by the Data Subject and, in order to prevent the unauthorised use of document(s) suitable for personal identification, to check, based on the data supplied by the any authority under a legal regulation, or from any other publicly accessible database, the provided personal data, the documents presented, the photo and signature of the person acting on the Data Subject's behalf, the reason, date and time of deletion, if any, from the records, and to request valid data from the records on the basis of the personal identification data in the course of the then-current banking transaction and in the action taken for the collection of a claim, if any, originating from such transaction.

8.4. Handling and copying of documents

The Controller shall be entitled, for the purpose of providing the services under the contracts, checking compliance with the Data Subject's obligations and fulfilling the Controller's commitments, request, either electronically or by telephone, as well as verify and store, any information related to the Data Subject's identity, deposit, credit and risk data, and the documents containing such information. The documents supplied – except for the documents submitted electronically – must be either originals or copies authenticated by a notary public.

If the Data Subject consents, or legal regulations require, when certain financial products are requested, the Controller shall make copies of the applicant's photo identity document, and the copy may be processed until the transaction exists.

8.5. Data processing performed for the purpose of risk avoidance and management

The Controller shall be entitled, before concluding the service contract, to check the risks associated with providing the service to the party who wishes to enter into a contract (prospective customer). To this end, the Controller is entitled to ask the Data Subject to submit, for the purpose of risk assessment, data and documents, which the Controller may analyse and check, and it is also entitled to use the available databases for purposes of analysis and checking.

8.6. Data processing performed for prevention of money laundering and terrorism financing

Based on the legal regulations on the prevention of money laundering and terrorist financing, the Controller carries out the identification of customers, and, in the cases and in the manner specified by the law, it provides data to third parties and authorities. Such data processing qualifies as compulsory data processing based on the legal regulations; the general contractual conditions provide information on this.

8.7. Processing of certain identifiers

The Controller is entitled to process the identifiers that are necessary for the fulfilment of obligations stipulated by the legal regulations. If such a legal relationship is established between the Data Subject and the Controller in relation to which the Controller incurs a tax-payment obligation – including the related data reporting obligation – the Bank may process the Data Subject's tax ID code.

8.8. Data processing performed by CIB Internet Bank and e-Broker

During the use of CIB Internet Bank and e-Broker the Customer contacts the Bank, as Controller, via the internet. In such case the Bank is entitled to process all the data that is required for identification and for the establishment and maintenance of a secure connection, including in particular any data related to the IT tools used by the Customer, and to access, that have been made available to the Bank.

8.9. FATCA

Based on the FATCA Act, the Bank carries out the identification of customers, and, in the cases and in the manner specified by the law, it provides data to third parties and authorities. Such data processing qualifies as compulsory data processing based on the legal regulations; the general contractual conditions provide information on this.

9. Duration of data processing

Personal data may be processed in a manner that permits identification of the data subject solely for the time required to achieve the purposes of processing.

The Controller retains the personal data available to it in line with the various purposes of processing and legal bases, in the case of a legal requirement, in accordance therewith. The retention period may be, in particular

a) in the case of processing based on the data subject's consent, the time until the withdrawal of the consent statement,

b) following the termination of the contractual relationship between the Controller and the data subject, the time until the end of the limitation period (unless otherwise stipulated by law),

c) in the case of statutory mandatory processing, until expiry of the statutory time limit; e.g. in connection with taxation, 5 years, in connection with accounting, as a general rule, 8 years.

The personal data of the Data Subject may be processed for direct marketing and research purposes until the date specified in the Data Subject's consent, but in any case no longer than until the withdrawal of the Data Subject's consent or notification of the Data Subject's objection according to section 7.

The Controller erases the data if it is obvious that such data will not be used in the future, that is, if the purpose of data processing has ceased.

10. Data protection impact assessment and prior consultation

10.1. Data protection impact assessment

Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the Controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

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

A data protection impact assessment shall in particular be required in the following cases:

a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

b) a systematic monitoring of a publicly accessible area on a large scale.

The assessment shall contain at least:

a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;

b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

c) an assessment of the risks to the rights and freedoms of data subjects; and

d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

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

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

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

10.2. Prior consultation

The controller shall consult the supervisory authority prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.

When consulting the supervisory authority, the Controller shall provide the supervisory authority with:

a) where applicable, the respective responsibilities of the Controller, joint controllers and processors involved in the processing, in particular for processing within a group of undertakings;

b) the purposes and means of the intended processing;

c) the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to this Regulation;

d) where applicable, the contact details of the data protection officer;

e) the data protection impact assessment; and

f) any other information requested by the supervisory authority.

11. Data transfer

11.1. General rules of data transfer

The transfer of data may in all cases take place only on the basis of appropriate legal grounds.

The Controller fulfils regular data reporting tasks to the organisations specified in the law, at the intervals and with the content specified in the law. The Controller only transfers personal data if the legal grounds for doing so are clear, and if the purpose of such transfer and the recipient of the transferred data are precisely defined. The Controller always documents the data transfer, ensuring that the procedure and legitimacy of the transfer may be proven. Appropriately and officially issued documents containing the request for data provision and those providing for the fulfilment of such request are primarily used for documentation purposes.

The Bank, as Controller, is obliged to perform any data transfer that is stipulated by law.

In addition to the above, personal data may only be transferred if the Data Subject has expressly consented to it. In order to ensure that such consent can be subsequently verified, it must, if at all possible, be made in writing. The requirement to have such consent in writing may be ignored if the data transfer is of little consequence as regards the recipient, the purpose of the transfer or the type of data involved. If the data transfer is subject to the consent of the Data Subjects, the Data Subject shall only give his/her consent if he/she is aware of the recipient and the purpose of the data transfer.

The above bans and limitations shall also apply after the end of the customer relationship.

11.2. Provisions on bank secrets and insurance secrets

All facts, information, know-how or data in the financial institution’s possession on clients relating to the person, data, financial standing, business activities, management, ownership and business relationships as well as the balance of and transactions executed on the account of a client at the financial institution as well as to his contracts entered into with the financial institution shall be construed banking secrets. For the purposes of the legal provisions pertaining to bank secrets, a 'customer' of the financial institution shall mean any person (entity) using the Bank's financial services.

If the Customer is a natural person, the personal data related to him/her shall qualify as a bank secret. The Bank shall only release a bank secret to a third party if

a) The Customer or his/her lawful representative requests it, with a precise indication of the range of bank secrets pertaining to him/her that may be disclosed set forth in a notarised deed or a private document with full probative force, or if he/she gives an authorisation for such. A notarised deed or a private document with full probative force is not necessary if the Customer submits this written declaration as part of the process of concluding a contract with the financial institution.

b) If the Credit Institutions Act grants an exemption from the obligation to keep bank secrets.

c) The financial institution’s interests require to sell its claim outstanding against the Customer or enforce an overdue claim.

Insurance secret is every data, not containing classified data, available to the insurer, reinsurer, insurance intermediary, insurance consultant, which refers to personal circumstances, assets or finances of the clients (including the damaged parties) of the insurer, reinsurer, insurance intermediary, insurance consultant, or their contract signed with the insurer or reinsurer.

A bank secret may only be disclosed to a third party if

a) The Customer or its legal representative has given a written release, precisely indicating the scope of insurance secrets that may be disclosed,

b) under the Act on Insurance Services, there is no obligation of confidentiality.

11.3. Regular data transfers

The Controller performs the following regular data transfers:

a) The Controller reserves the right to transfer its receivables to a third party by assignment, in compliance with the rules of the Civil Code. The person of the beneficiary changes as a result of such assignment. In the case of an assignment, the assignor Controller transfers the data related to the assigned receivables to the person who, by the assignment, is in the position of beneficiary.

b) The Controller transfer its customers' data in accordance with Act CXXII of 2011 to the financial enterprise (BISZ Zrt.) that manages the central credit information system (hereinafter: CCIS). The financial enterprise managing the CCIS transfers the data processed to third parties (reference data providers) in the manner defined by law. The Controller's general contractual conditions provide detailed information in respect of such transfer of data.

c) If the Data Subject gives the Controller such order on the basis of which the data transfer is necessary, the Controller may transfer the data for the purpose of executing the order, to the extent required for this purpose, and in this respect the Data Subject exempts the Controller from its obligation of confidentiality.

d) To fulfil obligations of reporting data to authorities and the court, the Controller transfers the data requested by the authority or the court.

12. Processing of data files

The Controller shall ensure that the manner and data content of the records always complies with the latest effective legal regulations. The types of data processing that are based on the legal regulations are mandatory, and the Data Subjects may request information on these. The Controller shall provide for the appropriate logical and if necessary, physical separation of the various types of data processing with different purposes.

The Controller processes the electronic and paper-based records based on uniform principles, with due regard to the characteristics resulting from the differences between data carriers within the records. The principles and obligations under this Policy are equally applied to both electronic and paper-based records.

The record containing the customer data and the record related to the services provided by the Controller are articulated in order to ensure that the data processing systems that can be separated by legal basis and purpose are indeed separated from each other. By defining the structure of the record-keeping system and the authorisations and through other organisational measures the Controller ensures that data in the records is only available to those employees and other persons acting within the Controller's sphere of interest who need this for their job and for the performance of their tasks.

The Controller ensures access to its records, subject to the fulfilment of the data security requirements, to those third parties collaborating as data processors who provide the Controller with services related to data processing.

The Controller's electronic records comply with the requirements of data security, and the records ensure that only persons who specifically need it for the performance of their tasks have access to the data, and only in relation to a specific purpose.

The Controller ensures that the principle of data minimisation is enforced.

12.1. Records of processing activities

The Controller shall maintain a record of processing activities under its responsibility. That record shall contain the essential circumstances of processing, in particular the following information:

a) the name and contact details of the controller and the joint controller, the controller's representative and the data protection officer;

b) the purposes of data processing;

c) a description of the categories of data subjects and of the categories of personal data;

d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;

e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers, the documentation of suitable safeguards;

f) where possible, the envisaged time limits for erasure of the different categories of data;

g) where possible, a general description of the technical and organisational security measures.

13. Data security

The Controller shall provide for the security of the data. To this end, it shall take all the necessary technical and organisational measures with regard to data stored on either IT devices or on traditional paper-based data carriers. To protect the data files processed electronically in various records, it must be ensured via appropriate technical solutions that the data stored in the records – unless permitted by law – cannot be directly linked and associated with the data subject.

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Controller shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

a) the pseudonymisation and encryption of personal data;

b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

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

The Controller shall take steps to ensure that any natural person acting under the authority of the Controller or the processor who has access to personal data only processes them in accordance with the Controller's instructions and the principle of purpose limitation. The Controller's records must ensure that only persons who specifically need it for the performance of their tasks have access to the data, and only in relation to a specific purpose.

The Controller provides for the enforcement of the rules on data security by way of separate policies, procedures and procedural rules. In order to fulfil the conditions of data security, it provides for the appropriate instruction of the employees concerned.

13.1. Protection of IT records

As part of its tasks related to IT security, the Controller primarily provides for the following:

- Measures ensuring protection against any unauthorised access, including the protection of software and hardware devices, and physical protection (access protection, network protection);
- Measures ensuring the possibility of recovery of the data files, including the preparation of regular backups and the separated, secure management of copies (mirroring, security backups);
- Protection of data files against viruses (virus protection);
- Physical protection of data and the related data carrier devices, including damage caused by fire, flood, lightning and other natural disasters, and providing for the possibility of recovery following instances of damage caused by the above events (archiving, fire protection).

13.2. Protection of paper-based records

The Controller takes all measures necessary for the protection of paper-based records, particularly with regard to physical security and fire protection.

Employees and other persons acting on behalf of the Controller shall be obliged to keep safe those data carriers used or possessed by them that also contain personal data, regardless of the method of data recording, and to protect the data against unauthorised access, change, transfer, publication, deletion or destruction and against involuntary destruction or damage.

13.3. Regulation of data security

The Controller provides for the enforcement of the data security requirements by way of separate policies and procedures. Its employees as well as the persons acting within the Bank's sphere of interest shall always act in accordance with the rules ensuring high-level enforcement of data security set out in separate policies and procedures.

13.4. Personal data breach

13.4.1. Handling personal data breaches

In the case of a personal data breach, the Controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

The processor shall notify the Controller without undue delay after becoming aware of a personal data breach.

The notification must at least:

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

Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

The Controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken.

13.4.2. Communication of a personal data breach to the data subject

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

The communication to the data subject shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures included in the notification referred to in section 13.4.

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

the Controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;

the Controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise;

it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

14. Data processor

14.1. General rules of data processing by the processor

The Controller may employ data processors in its activities, based on permanent or one-off mandates. Permanent data processing functions may primarily take place for the purpose of fulfilling administrative tasks related to customer service, service provision and the maintenance of the IT system.

The Controller shall, upon request, inform the Data Subjects of the details of the data processing activity, including in particular the executed operations and the instructions given to the data processor.

The data processor's rights and obligations regarding the processing of personal data are defined by the Controller, in accordance with the legal regulations. Responsibility for the lawfulness of the instructions related to data processing operations shall be borne by the Controller.

Within the scope of its activity and within the parameters defined by the Controller, the data processor is responsible for the processing, modification, erasure, transfer and publication of personal data. The processor may only use other processors according to the Controller's instructions.

The data processor may not make any specific decisions related to data processing; he/she may only process the personal data that comes to his/her knowledge in accordance with the Controller's instructions, he/she may not perform any data processing for his/her own purposes, and he/she must store and keep the personal data in accordance with the Controller's instructions.

The Controller ensures, by establishing appropriate contractual conditions and taking organisational and technical measures, that during the data processor's activity the rights of the Data Subjects may not be harmed or compromised, and that the data processor can only obtain any personal data if this is indispensable for the fulfilment of its duties.

The employment of a data processor is only possible on the basis of a written contract.

The contract must contain at least the following elements:

a) name of the controller and the processor;

b) subject, duration, type and purpose of the data processing;

c) categories of data subjects;

d) description of the data processing activity;

e) type and scope of personal data to be handed over;

f) in the case of automated data processing, the method used and its essence;

g) obligations and rights of the Controller and the processor;

h) the Controller's guarantee to the effect that the database and personal data handed over are processed legally;

i) representations of the data processor to the effect that it

ia) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

ic) shall take the data security measures that arise within the scope of its activity;

id) taking into account the nature of the processing, assists the controller by appropriate

technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights;

(ie) assists the controller in ensuring compliance with its obligations, taking into account the nature of processing and the information available to the processor;

if) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless the Hungarian law requires storage of the personal data;

ig) the processor's statement to the effect that it makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the Regulation, and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller;

j) prohibition of the use of data by the processor for its own purposes and purposes different than those specified in the contract;

k) the requirement that the processor, in the course of performing its activity – except for outsourcing specified by Section 68 of the Credit Institutions Act and joint processing – shall not be permitted to use other processors without the consent of the data controller ;

l) the processor's commitment to comply with data security rules;

m) the specification that the processor shall immediately inform the Controller if, in its opinion, an instruction infringes the Regulation or other Union or Member State data protection provisions.

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

14.2. Individual data processing cases

The data processors used by the Controller change constantly. The Controller provides information on the identity of the data processors on the www.cib.hu website.

15. Outsourcing

The Controller may outsource any activity that is related to its financial and supplementary financial service activity, or any such activity as is ordered to be performed by a legal regulation, that involves data processing by the Controller or a processor, or data storage, subject to compliance with the data protection provisions. It provides to the party performing the outsourced activity all the data related to the outsourced activity that is required for the activity to be carried out.

When selecting the party that will perform the outsourced activity, drafting and concluding the outsourcing agreement, and monitoring the performance of the outsourced activity, the Controller shall ensure that the protection of personal data by the party performing the outsourced activity is assured.

The Controller provides information regarding the outsourced activity and the parties performing such activity on the www.cib.hu website and in the general contractual conditions.

16. Automated individual decision-making, including profiling

In the case of automated decision-making, the Controller shall adopt its decisions that affect the Data Subject and his/her legal situation, through technical means via automated decision-making. Data required for this may be available through data disclosure by the Data Subject himself/herself, but data otherwise available about the Data Subject may also be used.

The Data Subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

The Controller is not obliged to ensure this right of the Data Subject if the decision:

a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;

b) is authorised by Union or Member State law to which the controller is subject; or

c) is based on the data subject's explicit consent.

In the cases referred to in sections (a) and (c), the Controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the Controller, to express his or her point of view and to contest the decision.

17. Instances of data processing related to the Controller's website

In relation to the www.cib.hu website, the Controller processes personal data on the basis of the "legal statement" published on the website. This statement provides information on all the data processing related to the website.

The data processing performed by CIB Internet Bank and e-Broker is governed by the provisions of this chapter of the Policy.

18. Rights of Data Subjects and the enforcement thereof

18.1. Right to receive information

18.1.1. Information to be provided where personal data are collected from the Data Subject

18.1.1.1. Where personal data relating to a Data Subject are collected from the Data Subject, the Controller shall, at the time of obtaining the personal data (concurrently with the data collection, at the latest), provide the Data Subject with all of the following items of information:

a) the identity and the contact details of the Controller and, where applicable, of the Controller's representative;

b) the contact details of the data protection officer, where applicable;

c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

d) where the processing is based on a legitimate interest, the legitimate interests pursued by the Controller or by a third party;

e) the recipients or categories of recipients of the personal data, if any;

f) where applicable, the fact that the Controller intends to transfer the personal data to a third country or international organisation, and the existence or absence of an adequacy decision by the European Commission, or reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or to where they have been made available.

18.1.1.2. In addition to providing the information referred to above, the Controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

b) the existence of the right to request from the Controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;

c) in the case of processing performed on the basis of consent, the existence of the right to withdraw consent at any time, which does not affect the lawfulness of processing based on consent before its withdrawal;

d) the right to lodge a complaint with a supervisory authority;

e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

f) the existence of automated decision-making, including profiling, and, at least in those cases, comprehensible information about the logic applied, as well as the significance and the envisaged consequences of such processing for the data subject.

Where the Controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the Controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in section 18.1.1.2.

The obligation to provide information shall not apply where and insofar as the Data Subject already has the information.

18.1.2. Information to be provided where personal data have not been obtained from the Data Subject

18.1.2.1. Where personal data have not been obtained from the Data Subject, the Controller shall provide the Data Subject with the following information:

a) the identity and the contact details of the Controller and, where applicable, of the Controller's representative;

b) the contact details of the data protection officer, where applicable;

c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

d) the categories of personal data concerned;

e) the recipients or categories of recipients of the personal data, if any;

f) where applicable, the fact that the Controller intends to transfer personal data to a recipient in a third country or international organisation, and of the existence or absence of an adequacy decision by the Commission, and a reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available.

18.1.2.2. In addition to the information, the Controller shall provide the Data Subject with the following information necessary to ensure fair and transparent processing in respect of the Data Subject:

a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

b) where the processing is based on the Controller’s legitimate interest, the legitimate interests pursued by the Controller or by a third party;

c) the existence of the right to request from the Controller access to and rectification or erasure of personal data or restriction of processing concerning the Data Subject and to object to processing as well as the right to data portability;

d) where the processing is based on the granting of consent, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

e) the right to lodge a complaint with a supervisory authority;

f) from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;

g) the existence of automated decision-making, including profiling, and, at least in those cases, comprehensible information about the logic applied, as well as the significance and the envisaged consequences of such processing for the Data Subject.

18.1.2.3. The Controller shall provide the information referred to in sections 18.1.2.1. and 18.1.2.2 as follows:

within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed;

if the personal data are to be used for communication with the Data Subject, at the latest at the time of the first communication to that Data Subject; or

if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

Where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the Data Subject, prior to such further processing, with information on that other purpose and with any relevant further information.

18.1.2.4. The information does not have to be provided where and insofar as:

a) the Data Subject already has the information;

b) obtaining or disclosure is expressly laid down by Hungarian law to which the Controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; or

c) the personal data must remain confidential subject to an obligation of professional secrecy regulated by European Union or Hungarian law (e.g. banking secrecy), including a statutory obligation of secrecy.

18.1.3. Right of access by the Data Subject

The Data Subject shall have the right to obtain from the Controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

a) the purposes of data processing;

b) the categories of personal data concerned;

c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

e) the existence of the right to request from the Controller rectification or erasure of personal data or restriction of processing of personal data concerning the Data Subject or to object to such processing;

f) the right to lodge a complaint with a supervisory authority;

g) where the personal data are not collected from the Data Subject, any available information as to their source;

h) the existence of automated decision-making, including profiling, and, at least in those cases, comprehensible information about the logic applied, as well as the significance and the envisaged consequences of such processing for the Data Subject.

Where personal data are transferred to a third country or to an international organisation, the Data Subject shall have the right to be informed of the safeguards relating to the data transfer.

The Controller shall provide the Data Subject with a copy of the personal data undergoing processing. For any further copies requested by the Data Subject, the Controller may charge a reasonable fee based on administrative costs, as set out in a separate policy. Where the Data Subject makes the request by electronic means, and unless otherwise requested by the Data Subject, the information shall be provided in a commonly used electronic form. The right to obtain a copy shall not adversely affect the rights and freedoms of others.

18.2. Right to rectification

The Data Subject may request the Data Controller to rectify one or more items of personal data that have been indicated incorrectly. Where regular data provision takes place on the basis of the data to be rectified, where necessary the Controller shall inform the recipient of the data about the rectification, and shall remind the Data Subject that the Data Subject must also initiate the rectification at other controllers.

18.3. Right to erasure, objection and the restriction of processing

18.3.1. Right to erasure ('right to be forgotten')

The Data Subject shall have the right to obtain from the Controller the erasure of personal data concerning him or her without undue delay and the Controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

b) the Data Subject withdraws the consent on which the processing is based, and there is no other legal ground for the processing;

c) the Data Subject objects to the processing, and there are no overriding legitimate grounds for the processing, or, without any investigation into whether such grounds exist, the Data Subject objects to the processing with regard to processing conducted for the purpose of direct marketing;

d) the personal data have been unlawfully processed;

e) the personal data have to be erased to comply with a legal obligation, prescribed by a European Union or Hungarian law, to which the Controller is subject;

f) the personal data have been collected in connection with the offer of information society services relating to a person who is a minor.

Where the Controller has made the personal data public and is under an obligation to erase the personal data, the Controller, taking into consideration the available technology and the cost of implementation, must take reasonable steps – including technical measures – to notify the controllers who are processing the personal data of the fact that the data subject has requested the erasure, by such controllers, of any links to, or copies or reproductions of, the personal data in question.

The right of erasure shall not apply insofar as the processing is necessary:

a) for compliance with a legal obligation that stipulates the processing of the personal data, applicable under European Union or Hungarian laws to which the Controller is subject;

b) for the establishment, exercise or defence of legal claims.

18.3.2. Right to object

The Data Subject shall have the right to object at any time, on grounds relating to his or her particular situation to the processing of personal data concerning him or her which is necessary for the pursuit of a legitimate interest of the Controller or a third party, including profiling based on the above mentioned provisions. In this event, the Controller shall no longer process the personal data unless the Controller demonstrates compelling legitimate grounds for the processing that override the interests, rights and freedoms of the Data Subject, or which are related to the establishment, exercising or defence of legal claims.

Where personal data are processed for direct marketing purposes, the Data Subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

Where the Data Subject objects to processing of the personal data for direct marketing purposes, the personal data shall no longer be processed for the purpose of profiling.

No later than at the time of the first contact with the Data Subject, the right referred to above shall be explicitly brought to the attention of the Data Subject and shall be presented clearly and separately from any other information.

In the context of the use of information society services, the data subject may exercise his or her right to object by automated means based on the appropriate technical specifications.

18.3.3. Right to restriction of processing

The Data Subject shall have the right to obtain from the Controller restriction of processing where one of the following applies:

the accuracy of the personal data is contested by the Data Subject, for a period enabling the Controller to verify the accuracy of the personal data;

the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

the Controller no longer needs the personal data for the purposes of the processing, but they are required by the Data Subject for the establishment, exercise or defence of legal claims;

the Data Subject has objected to processing in accordance with the provisions of the first paragraph of section 18.3.2.; in this case, the restriction shall apply until it is determined whether the legitimate grounds of the Controller override the legitimate interests of the Data Subject.

Where processing has been restricted on the basis of the above, such personal data shall, with the exception of storage, only be processed with the Data Subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest in the European Union or a Member State.

A Data Subject who has obtained restriction of processing on the basis of the above shall be informed by the Controller in advance of the lifting of the restriction on processing.

18.3.4. Notification obligation regarding rectification or erasure of personal data or restriction of processing

The Controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with sections 18.3.1-18.3.3. to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The Controller shall inform the Data Subject about such recipients at the request of the Data Subject.

18.4. Right to data portability

The Data Subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a Controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the Controller to which the personal data have been provided, where:

a) the processing takes place for one or more specific purposes or is based on the express consent of the Data Subject, or is necessary for the conclusion of a contract with the Data Subject, or the subsequent performance thereof; and

b) the processing is carried out by automated means.

In exercising his or her right to data portability in accordance with the above, the Data Subject shall have the right to have the personal data transmitted directly from one Controller to another, where technically feasible.

The exercise of the right to data portability shall be without prejudice to the right to erasure (“right to be forgotten”). That right shall not apply in cases where the processing is necessary for the performance of a task carried out in the public interest or in the course of exercising official authority vested in the Controller.

The right to data portability shall not adversely affect the rights and freedoms of others.

19. Data protection officer

The Controller employs a data protection officer, who is also the Controllers’ single data protection officer, insofar as any Controller does not independently employ or engage another data protection officer.

The single data protection officer: Dr. Vanda Toma

Phone: +36-1-423-2396

The Controller shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

The Controller shall support the data protection officer in performing the tasks by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.

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

Data Subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation.

The data protection officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Hungarian law.

The data protection officer may fulfil other tasks and duties. The Controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.

19.1. Tasks of the data protection officer

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

c) to inform and advise the Controller or the Controller's data processor, and the employees who carry out processing, of their obligations pursuant to the Regulation and to other European Union or Hungarian data protection provisions;

d) to monitor compliance with the Regulation, with other Union or Hungarian data protection provisions and with the policies of the Controller or Processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;

e) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to section 10.1;

f) to cooperate with the supervisory authority; and

g) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in section 10.2, and to consult, where appropriate, with regard to any other matter.

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

20. Implementation of Chapter I within the Controller's organisation

In the course of implementing this chapter of the Policy, the tasks and responsibilities of the individual organisational units and persons within the Controller are defined by the polices relating to the Controller's organisation, operation and activity. Coordination of the tasks related to implementation of this chapter of the Policy is performed by the data protection officer.

The rights of the Data Subject, and the exercising of such rights, are not affected by the Controller's organisational and operating conditions. If the Data Subject has any questions, complaints or reports to make in relation to data processing and the rights related thereto, he/she may contact the customer service desk or the internal data protection officer. The customer service centre and the data protection officer ensure that the questions, complaints and reports reach the appropriate organisational unit, and that the Data Subject receives a response to them within the deadline, and that the necessary action is taken.

The Controller also provides information about its contact details and how to contact the data protection officer on the www.cib.hu website.