Magyar Export- Import Bank Zártkörűen Működő Részvénytársaság [Hungarian Export-Import Bank Private Limited Company]

Magyar Exporthitel Biztosító Zártkörűen Működő Részvénytársaság [Hungarian Export Credit Insurance Private Limited Company]

File number: EX/75-9/2022
M/34-9/2022

CEO Directive No. K-9/2022

Data Protection and Data Security Regulations

Organisational unit responsible: Data Protection Officer

Effective date: 22 March 2022

Table of Contents

1. Purpose and areas of application of the regulations

1.1. Purpose of the regulations

The purpose of the data protection and data security regulations (hereinafter: "**Regulations"**) is to define the rules pertaining to the processing, transferability and destruction of personal data, as well as the protection of internal information, at Magyar Export-Import Bank Zártkörűen Működő Részvénytársaság and Magyar Exporthitel Biztosító Zártkörűen Működő Részvénytársaság (hereinafter together: "**Company"**).

The purpose of the Regulations is, furthermore, to define the operational rules with regards to the Company's records maintained in relation to the processing of personal data, to enforce the constitutional principles of data protection and the right to informational self-determination, as well as to ensure observance of requirements relating to data security, through the application of Act CXII of 2011 on informational self-determination and freedom of information (hereinafter: **"Freedom of Information Act"**) and of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (**"General Data Protection Regulation"**, **"Regulation"** or **"GDPR"**).

1.2. Scope of the regulations

The material scope of these Regulations covers all personal data and all data management and Data Processing involving the Personal Data of natural persons carried out at the Company – at its registered office, and its domestic and foreign representation offices – regardless of whether the data management or Data Processing is wholly or partially performed using computers (i.e. electronically) or manually.

The personal scope of these Regulations covers all senior officers of the Company, the chairperson and members of its Supervisory Board and Board of Directors, its employees, and persons employed under any other legal arrangement for the conduct of work, as well as any trainees performing their internship at the Company.

The personal scope of these Regulations also covers those persons who hold or process personal data while performing their tasks related to the activity of the Company under a contract concluded with the Company (Data Processors, or simply Processors).

With respect to the processing of data related to the performance of anti-money laundering tasks, the provisions of the latest effective CEO Directive on the Prevention and Combating of Money Laundering and Terrorist Financing shall apply.

If a data is also classified as protected data (business and/or bank secret or insurance secret), it must be classified in the strictest security class (5 according to Annex 2 of the Information Security Regulations) and be subject to the stricter legal confidentiality requirements corresponding to the data type. If there is any doubt as to which provisions of these Regulations should be applied to a particular item of data, the opinion of the Data Protection Officer shall be definitive in the matter.

Concerning the processing of classified data, including personal and special data processed within the scope of classified data, provisions of the current version of the Company's regulation on the processing of Classified Data shall apply.

1.3. Terms related to data protection

TERMS RELATED TO DATA

Data: Representation of information in a new form suitable for communication, interpretation or processing. Formalised representation of facts, concepts or instructions suitable for communication, display or processing by humans or automated devices.

Data Set: the totality of Data processed in a filing system, regardless of the form in which the data is presented and the method of storage.

Biometric data: any personal data obtained by specific technical procedures relating to the physical, physiological or behavioural characteristics of a natural person, which enable or confirm the unique identification of the natural person, such as a facial image or dactyloscopic data.

Criminal personal data: personal data relating to the data subject or that pertain to any prior criminal offence committed by the data subject and that is obtained by organisations authorised to conduct criminal proceedings or investigations or by penal institutions during or prior to criminal proceedings in connection with a crime or criminal proceedings.

Data concerning health: personal data related to the physical or mental health of a natural person, including data related to healthcare services provided to the natural person that reveal information about his or her health status.

Data Subject: any natural person identified or identifiable – directly or indirectly – on the basis of Personal Data.

Genetic data: any personal data relating to the inherited or acquired genetic characteristics of a natural person which contains unique information on the physiology or the health of that natural person and which is derived primarily from an analysis of a biological sample taken from that natural person.

Data of public interest: based on Section 3 (5) of the Freedom of Information Act, information or data other than personal data, registered in any mode or form, controlled by the Company and concerning its activities or generated in the course of performing its public tasks, irrespective of the method or format in which it is recorded, or of its single or collective nature, in particular data concerning the scope of authority, competence, organisational structure, professional activities and the evaluation of such activities covering various aspects thereof, the type of data held and the regulations governing operations, as well as Data concerning financial management and concluded contracts.

Data made public on the grounds of public interest: based on Section 3 (6) of the Freedom of Information Act, all Data which does not fall within the concept of Data of Public Interest, the disclosure, acquaintance or making available of which is required by law in the public interest. In accordance with Section 26 (2) of the Freedom of Information Act, the name of the person undertaking tasks within the scope of responsibilities and authority of the body undertaking public duties, as well as his/her scope of responsibilities, scope of work, executive mandate and other Personal Data relevant to the provision of his/her responsibilities to which access must be ensured by law qualify as data made public on the grounds of public interest. In accordance with Section 27 (3) of the Freedom of Information Act, as data made public on the

grounds of public interest, the following shall not qualify as business secrets: the budget of the central government and the local governments; furthermore, data related to the use of European Union funds, to benefits and allowances involving the budget, to the management, possession, use, utilisation and the disposal and encumbering of central and local government assets, and the acquisition of any right in connection with such assets, as well as data the accessibility or disclosure of which is prescribed on public interest grounds by a specific act.

Sensitive Data: all data belonging to specific categories of personal data, i.e. personal data referring to racial or ethnic origin, political opinion, religious or philosophical beliefs or trade union membership, as well as genetic data, biometric data for the unique identification of natural persons, health data and personal data relating to the sexual life or sexual orientation of natural persons.

Personal Data: any information relating to an identified or identifiable 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.

Main types of personal data:

a) *Natural identifier Data*: especially the name of the Data Subject, his or her mother's maiden name, place and date of birth, home address and/or place of residence.
b) *Artificial identifier Data*: Data generated by mathematical or other algorithms, especially the personal identification code, social security number (TAJ), tax identification number, ID card number, driving licence number, address card number, or passport number.

The Personal Data shall retain this quality during the Data Processing as long as its connection with the Data Subject can be restored. The connection with the Data Subject can be restored if the Company has the technical conditions necessary for such restoration.

Client: Clients defined in the Companies' Business Regulations in force at any time. The supplier and the supported party shall also be a client. A supplier is a natural person or business organisation that is in a contractual relationship with the Company for the sale of goods or the provision of services or is seeking such contractual relationship. A supported party is any natural person, business entity, organisation, association or foundation to which the Company provides or plans to provide support upon request or based on its own decision, for free, as well as a beneficiary from whom, in return for the support, the Company expects conduct of a non-financial nature that effectively publicises the Company's activity as sponsor, or with whom the Company is preparing to conclude a contract of such content.

TERMS CONCERNING RESPONSIBILITIES RELATED TO DATA PROCESSING

Data owner: the head of the organisational unit to which the legal regulation or the organisation regulating instrument governed by public law assigns the data processing, and/or where the data are generated

Data Controller or Controller: the natural or juridical person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. For data processing activities performed in accordance with these Regulations, the Company shall be the Controller.

Data Processor or Processor: the natural or juridical person who processes personal data on behalf of the data controller in accordance with its instructions.

Recipient: a natural or juridical person, public authority, agency or another body, to which the personal data is communicated disclosed, whether a third party or not. However, public authorities that may receive personal data in the context of a particular inquiry in accordance with EU or Member State law shall not be regarded as recipients; the processing of such data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

Third party: a natural or juridical person, public authority, agency or body other than the Data Subject, the controller, the processor or persons who, under the direct supervision of the controller or processor, are authorised to process personal data.

Authority: the Hungarian National Authority for Data Protection and Freedom of Information.

Unauthorised person: any person who is not entitled to know the Data.

TERMS RELATED TO THE PROCESSING OF DATA

Data processing or **processing**: any automated or non-automated operation or set of operations performed on Personal Data or data files, regardless of the procedure used, such as collecting, recording, registering, organising, segmenting, storing, transforming, changing, querying, viewing, using, communicating, transmitting, disseminating, disclosing, co-ordinating or interconnecting, deleting and destroying, as well as preventing the further use of the data. Data processing also includes the taking of photographs, sound or image recordings, as well as the recording of physical characteristics (e.g. fingerprints or palm prints, DNA samples, or iris scans) that can be used to identify a person. The special rules concerning the IT system with regard to the protection of electronically processed Data are contained in the Information Security Regulations and the Regulations on the Functioning of IT Operations.

Restriction of data processing: the marking of stored personal data with the aim of restricting its processing in the future.

Data destruction: the complete physical destruction of the data medium that contains the Data.

Data transfer: making the Data available to a specified Third Party.

Data erasure: making the Data unrecognisable in such a way that its restoration is no longer possible.

Pseudonymisation: the processing of personal data in such a way that it is no longer possible to determine to which specific natural person the personal data relates without the use of additional information, provided that such additional information is stored separately and that technical and organisational measures are taken to ensure that this personal data may not be linked to identified or identifiable natural persons.

Original purpose: the purpose for which the personal data was collected.

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

Legitimate interest: the legitimate (business) interest of the Company or a third person which overrules the basic rights and freedoms of the Data Subject(s), and which shall apply when data processing is carried out for a legitimate purpose other than for the performance of a contract concluded or to be concluded with the Data Subject, in the vital interest of the data subject or for compliance with a legal obligation.

Joint data processing: the determining of the purposes and means of data processing jointly, by two or more controllers.

Transfer of data abroad: transfer of Personal Data to a third country or to an international organisation, including the re-transfer of Personal Data from a third country or international organisation to another third country or to another international organisation.

Disclosure: making the Data available to anyone.

Profiling: 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.

TERMS RELATED TO DATA SECURITY

Personal data breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised release of, or unauthorised access to, Personal Data transmitted, stored or otherwise processed, thus especially unauthorised access, alteration, transfer, disclosure, erasure or destruction, as well as accidental destruction or damage (e.g. physical or virtual break-in, Data Processing without authorisation, unauthorised access).**Security:** the state of the system to be protected is adequate for the organisation, and provides closed, full and continuous protection proportionate to the risks.

Threat (danger): any operation or event, or the lack of such operation or event, which may endanger protection or Security.

1.4. Types of data

The following types of data classified by law occur at the Company:

- Personal data (including the data of people acting on behalf of Clients, Suppliers and Supported Parties, as well as of Employees, and data specified in property declarations),
- business secret,
- bank secret.
- insurance secret.
- Data classified in accordance with Act CLV of 2009 on the Protection of Classified Information (only in the form of paper-based documents)
- other data stored in the IT system, but not categorised based on its data content.

2. Regulations concerning the protection of personal data

2.1. Legal regulations

Regulations and recommendations related to the protection of personal data:

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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 ("**Regulation**" or "**GDPR**")
- Act CXII of 2011 on Informational Self-Determination and Freedom of Information ("**Freedom of Information Act**");
- Act CXXII of 2011 on the central credit information system;
- Act XLII of 1994 on Magyar Export-Import Bank Részvénytársaság and Magyar Exporthitel Biztosító Részvénytársaság ("**EXIM Act**");
- Government Decree 85/1998 (V.6.) on the Interest Equalisation System of Magyar Export-Import Bank Részvénytársaság;
- Ministry of Finance Decree 16/1998 (V.20.) PM on the detailed rules on settlement with the central budget by the Magyar Export-Import Bank Részvénytársaság and Magyar Exporthitel Biztosító Részvénytársaság;
- Decree 54/2021 (XI. 23.) MNB on the reporting obligations to be fulfilled towards the central bank information system primarily in the interests of the performance by the National Bank of Hungary of its basic duties;
- Act CCXXXVII of 2013 on Credit Institutions and Financial Enterprises ("**Credit Institutions Act**");
- Act CXCV of 2011 on public finances ("**Public Finances Act**");
- Act CXXXIX of 2013 on the National Bank of Hungary;
- Act LIII of 2017 on the prevention and combating of money laundering and terrorist financing;
- Act V of 2013 on the Civil Code of Hungary (**"Civil Code"**);
- Act I of 2012 on the Labour Code ("**Labour Code**");
- Act LXXX of 2019 on the entitlement to social security benefits and the funding for these services ("**Social Security Act**");
- Act CXVII of 1995 on Personal Income Tax ("**Personal Income Tax Act**");
- Act CXXXIII of 2005 on the Rules for Security Services and the Activities of Private Investigators ("**PI Act**");
- Decree 41/2015 (VII 15) BM of the Ministry of the Interior on the requirements for technological security and secure information devices and products specified in Act L of 2013 on the electronic information security of state and local government bodies, as well as for classification into a security class and security level;
- Government Decree No. 451/2016 (XII.19.) on detailed rules regarding the operation of the electronic public procurement system;
- Ministry of Economy and Transport Decree 1/2018 (XII.29.) ITM on the rules of digital archiving;
- Act CLV of 2016 on Official Statistics;
- Act CLII of 2007 on the obligations of submitting declaration of assets and liabilities;
- Recommendation 27/2018 (XII. 10.) of the National Bank of Hungary on the establishment and operation of internal defence lines and the governance and control functions of financial organisations;
- Recommendation 8/2020 (VI.22.) of the National Bank of Hungary on the protection of the IT system.

2.2. Internal regulations

The Company's applicable and effective:

- Organisational and Operational Regulations *("OOR"*);
- Organisational Charts ("*OCh*");
- Business Regulations;
- Regulations on Property Declarations;
- Compliance Regulations;
- Records Management Regulations;
- Information Security Regulations ("*ISR*");
- Business Continuity Framework Regulations;
- Physical Security Regulations;
- Fire Safety Regulations;
- Ethical Codes;
- Regulations on the exercise of signatory rights;
- Outsourcing Policies;
- Term and content of personal materials and their management policy;
- Regulations on loans that may be provided to employees;
- Security regulations for the protection of classified information
- Internal Audit regulations;
- Regulations on the functioning of IT Operations;
- Regulations on the Procedure for internal regulation;
- Event and incident management regulations;
- Development and Change Management Regulations.
- Magyar Export-Import Bank Zrt.'s Directive on the Prevention and Combating of Money Laundering and Terrorist Financing;
- Magyar Export-Import Bank Zrt.'s Rules of Procedure for Lending;
- Rules of Procedure for Full and Unconditional Payment Guarantees Issued by the Rural Credit Guarantee Foundation of Magyar Export-Import Bank Zrt.;
- Procedure of tied aid lending of Magyar Export-Import Bank Zrt.;
- Procedure for ensuring tied aid loans of Magyar Exporthitel Biztosító Zrt.;
- Procedure for direct loans disbursed as part of the Compensation Loan Program of Magyar Export-Import Bank Zrt.;
- Client Due Diligence Regulations of Magyar Exporthitel Biztosító Zrt.:
- Regulations of Magyar Exporthitel Biztosító Zrt. on procedures related to international commitments;

3. Levels of data protection

3.1. Chief Executive Officer: has prime responsibility for data protection at the Company

His/her tasks:

- ensure effectiveness of the principles concerning the processing of personal data;
- ensure lawfulness of instructions related to data processing operations;
- ensure security of data, implementation of necessary organisational and technical measures, establishment of rules of procedure;
- ensure careful and clear separation of activities and responsibilities related to data protection;
- provide resources necessary for the tasks specified in the Data Protection and Data Security Regulation;

- appoint the Data Protection Officer in accordance with the provisions of the GDPR;
- in the case of unauthorised data processing and taking into account the recommendation of the Data Protection Officer, implement necessary measures.

3.2. Data Protection Officer

The Data Protection Officer shall act in matters falling within the scope of this Regulation.

The Data Protection Officer shall act independently in matters specified in this Regulation. The Data Protection Officer shall be appointed by the Chief Executive Officer, and shall directly report to him. The name and contact details of the Data Protection Officer shall be included in Schedule 1 of this Regulation.

Tasks of the Data Protection Officer:

- cooperation and provision of support in decision-making related to data processing and enforcement of the Data Subjects' rights;
- ensure compliance with regulations concerning data protection, this Regulation, as well as the provisions of other internal regulations related to data protection and data security, and data security requirements;
- promote the exercise of rights available to Data Subjects, and examine complaints sent to the Company in the case of unauthorised Data Processing, inform the Chief Executive Officer thereof and request the competent organisational unit to terminate such practice, and initiate the implementation of measures at the Chief Executive Officer;
- prepare and update this Regulation and harmonise it with other internal regulations;
- provide professional support to the Chief Executive Officer in the implementation of organisational measures necessary for the safe processing of data, establishment of rules of procedure;
- support with professional advice and monitor the performance of data protection impact assessments,
- provide opinion on other internal regulations before their disclosure from data protection prospective;
- provide opinion on IT developments from data protection prospective
- identify data protection risks
- monitor compliance with this Regulation and inform the Chief Executive Officer thereof in writing;
- continuously monitor international and Hungarian legislation related to data protection, and if necessary, initiate the modification of this Regulation and related internal regulations
- maintain the records of processing activities under Article 30 of the GDPR[1]

[1] Each controller shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:
a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;
b) the purposes of the 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 referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;
f) if possible, the deadlines assigned for erasing the different categories of data;

- provide up-to-date information concerning legal requirements concerning the processing of personal data and, if necessary, provide advice with respect to the means of their enforcement to the employees of the Company;
- provide new employees or, in the case of material changes, all the employees with training on data protection (see Chapter 16);
- report to the CEO on issues related to data protection and data security;
- evaluate findings of external and internal controls related to data protection, and, if necessary, initiate the implementation of measures with the CEO;
- retain documents and records generated in relation to Data Processing in accordance with the Document Management Regulation of the Company.
- cooperate with bodies and persons entitled to perform procedures related to the lawfulness of data processing, in particular keep contact with the Supervisory Authority in order to support preliminary cooperation and procedures performed by the Supervisory Authority
- during the term of his legal relationship and after its termination, the data protection officer shall keep secret the personal data, classified information and data qualified by an Act as protected secret or as a secret linked to exercising a profession that he has become aware of in the context of performing his activity, as well as all data, facts or circumstances that the controller or the processor employing him is not obliged to make publicly accessible according to the provisions of an Act.

During performance of his tasks related to monitoring, the Data Protection Officer shall monitor compliance with data protection regulations, in particular with respect to the practices, regulations and contracts applied by the Company, including agreements concluded with data processors.

3.3. Managers of the organisational units

Their tasks:

- ensure compliance with data protection requirements within their organisational units,
- cooperate with the Data Protection Officer in the examination of complaints;
- consult the Data Protection Officer in the case of disputes.

3.4. Chief Information Officer

His/her tasks:

- provide professional support to the Chief Executive Officer in cooperation with the head of Information Security in the implementation of technical organisational measures necessary for the security of electronic data, the establishment of the rules of procedure;
- ensure operation of the IT infrastructural background necessary for data security;
- submit professional recommendations to the CEO for the purchase of new IT resources related to data security
- consult the Data Protection Officer with respect to IT developments.

g) if possible, a general description of the technical and organisational measures referred to in Article 32(1).

3.5. Employees

Their tasks:

- within the scope of confidentiality undertaken in a statement – all Employees whose duties require to have access to Personal Data shall be responsible for their confidentiality in accordance with their classification (see the confidentiality related to data considered as business secret in accordance with the current version of the Compliance Regulation) and shall comply with the provisions of this Regulation;
- They shall not make any substantial decision concerning data processing, shall process Personal Data available to them exclusively to the extent specified in the effective instructions of the CEO, and may not carry out data processing for their own purposes;
- they shall store and retain Personal Data in accordance with the effective instructions of the CEO;
- they shall transfer notifications, requests related to Data Processing as well as complaints and objections submitted by the Data Subjects in relation to the processing of their Personal Data to the Data Protection Officer;
- they shall immediately report to their line manager and/or in accordance with Schedule 3 of this Regulation to the Data Protection Officer if they experience an incident or event related to the Personal Data, or its consequences, or if they believe that their occurrence is plausible, or if the provisions of this Regulation may not be enforced for any reason.

4. Data processed by the Company

4.1. Principles of Data Processing

The Company, as the data controller, is responsible for compliance with the data protection rules and for ensuring its ability to prove such compliance.

The Company acts in accordance with the requirements of good faith, fair procedure and transparency with regard to Data Processing, in cooperation with the Data Subjects. The Company shall exercise its rights and obligations related to Data Processing for the purposes intended, lawfully, and in a manner transparent to the Data Subject.

During the Data Processing, the Company shall ensure the accuracy, completeness and – if necessary for the purpose of the Data Processing – the up-to-date nature of the Data, and that the Data Subject may be identified only for the time necessary for the purpose of the Data Processing. In addition, it shall take all reasonable steps to delete or rectify personal data that are inaccurate or out of date for the purposes of the data processing, without delay.

Personal data may only be collected, stored, processed and transferred for specified, explicit and legitimate purposes and may not be used for other purposes in a manner that is incompatible with the original purpose. The Company continuously examines the purposes and means of data processing to ensure that these are appropriate, relevant, necessary and proportionate. The Company shall document this activity in an appropriate manner.

Personal data is stored by the Company in a form that allows the identification of the Data Subjects only for the time necessary to achieve the purposes of the processing of the personal data; the personal data may be stored for a longer period only if the Company is bound by law to process the personal data, or the personal data is being processed for the purpose of archiving in the public interest, for scientific and historical research purposes or for statistical purposes in accordance with Article 89 (1) of the GDPR.

The Company shall ensure implementation of technical and organisational measures necessary and appropriate for the data processing in order to ensure protection against unauthorised or unlawful processing of data, accidental loss, destruction or damage.

The Company shall process personal data in such a way that the rights of Data Subjects, as well as the integrity and confidentiality of the data, are ensured at all times.

The Company shall not apply decision-making or profiling based on automated processing concerning the categories of personal data and/or natural persons.

4.2. Purposes of the processing of personal data

The Company may process personal data exclusively for the originally specified purposes of data collection, in order to exercise its rights or perform its duties, and for other related purposes subject to the conditions set forth in this section.

Personal data may be collected, used, stored or otherwise processed if it is necessary for the following purposes:

a) it is ordered by law,
b) **in order to ensure responsible, effective and efficient business management, especially with regard to the following activities**:
    i. the pre-contract assessment of clients, the fulfilment of the contract signed or to be signed with the client, suppliers or supported parties, the conclusion and performance of financial transactions and insurance contracts, maintaining contact with clients and other contractual partners, fulfilling requests for further information submitted by clients, Data Subjects, suppliers or supported parties, or for enforcing their legal claims;
    ii. nurturing business and client relationships, managing system-level usernames and passwords, maintaining and expanding existing contacts with clients, suppliers and supported parties, and for statistical and scientific purposes;
    iii. implementing business processes, organisational and asset management, conducting internal audits and inspections, carrying out financial and accounting tasks, processing management reports and reviews;
    iv. for security reasons, in particular for asset protection reasons, and in order to identify the Data Subjects, clients or suppliers and determine their access rights;
    v. activities necessary for pursuing the legitimate interests of the Company or any third party;
    vi. fulfilment of legal obligations.

c) for the supporting of activities related to the security of the operation of the financial intermediary system, including the following activities:
    i. identifying, preventing and investigating activities that may have a negative effect on the Company, including, in particular, any misuse of the Company's products, services or facilities, (ii) any illegal or otherwise detrimental (planned) activity, or (iii) any violation of the (legal) regulations;
    ii. preventing, deterring or detecting a criminal offence or misconduct planned or committed against the financial intermediation system, the Company, the Data Subjects or the employees;
    iii. operating security and alerting systems used by the participants in the financial intermediation system; or
    iv. for the performance of legal obligations, especially with respect to obligations

related to the prevention of money laundering and terrorism.

If a question arises as to whether the processing of Personal Data in the interest of the above purposes is lawful, the opinion of the Data Protection Officer should be sought in writing by the organisational unit carrying out the processing, before the start of the data processing. The Data Protection Officer shall send a response to the request, in writing, within 3 (three) working days.

4.2.1. Processing of sensitive data

The Company may process sensitive data only for the purpose and to the extent necessary for the purpose specified in this section.

Sensitive data may only be collected, used or otherwise processed for one or more of the following purposes:

a) **Personal data revealing racial or ethnic origin** – The Company may process CCTV footage (i) for the purpose of identifying Data Subjects, business partners or suppliers; (ii) for security purposes; and/or (iii) in the interest of fulfilling a legal obligation;
b) **Criminal data** – (including data related to unlawful conduct or data retrieved from the criminal records):
   i. in the interest of the protection of the Company, the financial intermediary system and the employees crimes committed and, in the case of a suspicion of perpetration, against crimes contemplated;
   ii. in the interest of the protection, security and integrity of the Company, the financial intermediary system and the employees;
   iii. in the interest of the fulfilment of a legal obligation (including especially requirements related to the prevention of money laundering and terrorism).

c) **Biometric data** – The Company performs identification relating to Data Subjects on the basis of characteristics that allow unique identification; (ii) for security reasons; and (iii) processes such data in order to fulfil a legal obligation

In addition to the above processing purposes, sensitive data may only be processed under the following circumstances:

a) the Data Subject has given his or her explicit consent to the processing of the sensitive data;
b) in relation to sensitive data specifically disclosed by the Data Subject;
c) it is possible or mandatory under an applicable legal regulation;
d) it is necessary for the establishment, exercise or defence of legal claims;
e) it is necessary in order to protect the vital interests of the Data Subject, if it is not possible to obtain the Data Subject's prior consent.

If sensitive data is processed based on the consent of the Data Subject, the data processing may take place with the prior approval of the Data Protection Officer. The organisational unit carrying out the Data Processing shall request the approval of the Data Protection Officer in writing. The Data Protection Officer shall send a response to the request, in writing, within 3 (three) working days. Issued licenses shall be filed by the Data Protection Officer and shall be stored centrally in order to ensure transparent data processing of the organisation.

4.3. Rules concerning the processing of Employees' Personal Data

4.3.1. Purpose of the processing of Employees' Personal Data

The Company as Employer may process the Personal Data of the Employees exclusively for the original purposes of data collection. The Employer may process the personal data of its Employees for other purposes (such as: administration related to participation at leisure activities) or if there is an appropriate legal ground for processing, and only after provision of information under the terms set forth in Section 11 and, if necessary, after obtaining the Employee's consent.

The Employer shall collect, use, store or otherwise process personal data of the Employees for the following purposes:

a) **Human resources and organisation management**: data processing necessary for the performance of the employment contract or any other contract concluded with the Employee (or necessary for certain steps upon the Employee's request before conclusion of the contract) or for the administration of recruitment, selection or foreign mission, benefits, payments, career and talent management, performance evaluation, training, travel and reimbursement, employee communication, international assignments and litigation; or
b) **Performance of electronic business processes and internal management**: workflow management, registration of working hours, management of the assets of the Company, performance of internal audits and assessments; implementation of business controls, ensuring effective electronic communication; or
c) **Health and safety**: activities related to health and safety, protection of the assets, reputation of the Company, and the Employees, management of access rights and checking compliance with the regulations of the Company, or
d) **Organisational assessments and executive reports**: Performance of employee surveys, data processing necessary for executive reports and assessments; or
e) **Compliance with legal requirements**: compliance with legal requirements, sector-specific rules; or
f) **Protection of the vital interests of Employees**: Data Processing is necessary for the protection of the vital interests of the Employees.

4.3.2. Legal ground for the processing of Employees' data

The Company may process the Personal Data of Employees in the following cases:

a) if data processing is necessary for the conclusion of the employment contract or completion of the employment relationship;
b) if processing is necessary for compliance with a legal obligation
c) if processing is necessary for the enforcement of the legitimate interest of the Employer or any third party.
d) processing of Personal and Sensitive Data falling within the scope of national law in accordance with the law by ensuring purpose limitation and necessary extent of Processing specified therein

In view of the above, the legal basis for the Company's data processing with respect to Employee Data is Article 6(1) of the GDPR:

- a) (data processing based on consent),
- b) (data processing required for the performance of a contract),

- c) (mandatory data processing required to fulfil a legal obligation),
- f) (data processing necessary to enforce a legitimate interest).

If the planned data processing is necessary for the enforcement of the legitimate interests of the Employer or any third party, the organisational unit responsible for the processing shall consult the Data Protection Officer in order to identify the legitimate interest of the data controller and perform the interest assessment test in accordance with the Data Protection Regulation. The planned data processing may only be commenced if based on the interest assessment it may be stated that the interests of the data controller related to data processing are not overridden by the rights and freedoms of the Employee or any other person.

4.3.3. The Employee's consent

In the absence of the legal grounds set forth in Subsections a)-c) of the above section, in exceptional cases, the processing of the Employees' Personal Data may be based on the Employee's consent if the processing is not closely related to the employment relationship. If the employee refuses the consent, it may have no consequences detrimental to the Employee with respect to the employment relationship or any other work relationship. The organisational unit responsible for processing shall request the opinion of the Data Protection Officer on the planned processing before commencement of the processing which is based on the Data Subject's consent. The Data Protection Officer shall examine the planned processing, with special regard to the consequences the Employee may face if he or she refuses the consent, and shall send his or her opinion within three (3) working days to the organisational unit responsible for data processing.

The Employees are not obliged to consent to the processing of their Personal Data, and may withdraw their consent at any time, however, the withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. It shall be as easy to withdraw as to give consent. If the processing occurs explicitly based on the Employee's request (such as: the Employee wishes to use a service /employer loan/ provided by the Employer but not strictly related to the employment relationship or other work relationship, then it is not necessary to obtain a separate consent for the processing of personal data related to the use of such services or the conclusion of the contract), his or her consent to the data processing shall be considered as given if the Employee has received appropriate information on the circumstances of processing before commencement of such processing by the Employer.

The Company shall inform the Employees on the circumstances of Data Processing via the Notice for Employees on Data Processing in accordance with Schedule 5. Human Resources is responsible for the completeness of the information and retention of the copy of the information certifying its delivery in accordance with the rules of the instruction concerning the definition, content and management of Personal files.

The organisational unit responsible for data processing shall be responsible for obtaining the consent concerning data processing in a justifiable manner.

4.3.4. HR records

The HR records shall contain the personal data of any and all Employees. Personal data shall be used for the establishment of facts related to the work relationship, certification of job requirements and statistical data provision required by law.

The HR Records shall be maintained by the head of Human Resources and the employees of

Human Resources. The head of HR and its employees shall ensure security of data in the HR records and prevention of unauthorised access, whereas provision of physical and IT protection shall be the task of the head of Bank and Information Security concerning the totality of the payroll and employment records in accordance with the relevant instructions of the CEO.

Data of the HR records shall be provided by the Employee or the Company. The primary data registration shall take place when the work relationship is created.

As a prerequisite for establishing the employment relationship or other work relationship with the Company, upon establishment of the employment relationship, the Employee shall make a written statement as per Schedule No. 6 according to which he or she has become aware of this Regulation, and this statement shall be stored by the Human Resources. If the statement is not submitted within eight (8) days, it shall be considered as material breach of the obligations arising from the employment relationship. The Human Resources shall store the statement together with the personal file. If there are obstacles to the obtaining of the statement, the Data Protection Officer shall be immediately notified thereof, and the measures specified by him or her shall be implemented.

Within the organisation of the Company, data provision from the HR records may only be performed upon written request (email) for the CEO, and the heads of the organisational units/sub-units with respect to data necessary for the performance of executive tasks and the organisational unit managed by them. The Data Protection Officer and the employee of the Internal Audit may consult the personal files – based on request submitted to the head of Human Resources, with justification – while employees may consult their own personal files to the extent required and justified for the performance of their tasks.

4.3.5. Payroll and employment records

The payroll and employment records shall include the Personal Data of Employees and members of the Supervisory Board and the Board of Directors not having a work relationship with company related to the payroll of their salary and other income.

The payroll and employment records shall be maintained by the head of Human Resources and the employees of Human Resources. Physical protection of the payroll and employment records shall be ensured in accordance with the Physical Security Regulation. Electronic information security of electronically processed Personal Data shall be ensured in accordance with the IT Security Regulation. Performance of HR tasks set forth in the above instructions shall be ensured by the head of Human Resources, whereas provision of physical protection shall be the task of the head of Bank and Information Security, while the operation of IT security enforced according to the requirements of electronic information security shall be the duty of the IT Security director according to the relevant instructions of the CEO. Furthermore, the head of Human Resources shall comply with confidentiality requirements and cause others to do so in order to prevent unauthorised access.

Within the organisation of the Company, data provision from the payroll and employment records may only be performed for the CEO, and the heads of the organisational units/sub-units upon e-mail request with respect to data necessary for the performance of executive tasks and the organisational unit managed by them, except for personal data and data accessed with NEXON management rights. Therefore, it is not necessary to require prior writing, if the data provision is carried out on the platform of the management module set up in the electronic personnel system with differentiated access rights, by logging the Data Processing. The Data Protection Officer and the employee of the Internal Audit may consult the personal files upon

justified written request (email) sent to the head of Human Resources, while employees may consult their own personal files at any time.

4.4. Workplace monitoring of Employees

The Company shall and/or may monitor Employees with respect to their employment relationship based on legal regulation and its legitimate interest. During the monitoring of Employees, the Company and the Employee participating in the monitoring shall respect the human dignity and privacy of Employees subject to the monitoring. With respect to the workplace monitoring, the Employees are entitled to the rights under Section 12 of this Regulation which may be enforced as specified therein. The Employees shall be informed on the technical means applied during the workplace monitoring when they are hired.

4.4.1. Monitoring of electronic mail

Based on its legitimate interest related to the workplace monitoring, the Company is entitled to monitor the electronic mail of the Employees with technical means, for data security purposes and with respect to all employees on a regular basis, and in addition by adopting a gradual approach, if necessary, individually, in accordance with Information Security Regulations on the rules of electronic mail and instant messaging. In accordance with this Regulation, the Data Protection Officer shall perform controls related to the processing of personal and sensitive data.

If it becomes necessary to individually monitor the electronic mail, the Company may consult the emails outside the 'Private' folder in the account assigned to the Employee without limitation for work purposes, and if there is a 'Private' folder, then it may only consult the emails in that folder in exceptional cases which are duly justified, and by applying a gradual approach, mainly confining itself to the header and the recipient. If the Employer fails to achieve the purpose of the control by checking the header of the electronic mails contained in the 'Private' folder, then after checking the header and the recipient, it is entitled to request the Employee to hand over/present the content of the mail, and shall specify the purpose and expected result of the control, and shall immediately inform data subjects affected by the mail but not having a legal relationship with the Employer on the purpose, content, result of the control and any other relevant circumstances. The Employee may refuse to hand over the mail if it results in the violation of a third person's right to confidentiality of correspondence. Detailed monitoring of private mails may only occur if it is performed by the competent person of the investigating authority, if the control performed in accordance with the above was unsuccessful. The Company is not entitled to consult the private correspondence of Employees and natural persons affected by the private correspondence but not having a legal relationship with the Company.

Provision of data from the correspondence log may be requested in a notice containing the approval of the CEO, by the Data Protection Officer, head of Internal Audit, head of Bank and Information Security, IT Security Officer, and – to comply with a data request from an authority or the court, the head of Compliance and the head of the Legal department, also informing the CEO of this. The request shall indicate the user, the period in question, the direction of the correspondence, the email address of the partner (if emails from and to only one address are needed, and the address is known), or range (the domain of the known partner's e-mail address "@domain.country or functional_sign"), as well as the reason for the request and its legal basis. Employees of the Bank and Information Security are entitled to perform the control, and they are entitled to involve the Data Protection Officer if Personal and Sensitive Data are affected.

During the control, the Employee shall be present, unless his or her presence would undermine the purpose of the control, or if it is impossible, or if the limitation of the Employee's rights relating to the personality is allowed for in the law. If the Employee is permanently not at his or her workplace, and his or her account shall be checked, the Employee may appoint another Employee to view his or her account. If it is clear that the subject of a mail is official, then it may be handed over to the Company. If there is no appointed Employee, or he or she is not present at his or her workplace, the IT specialist responsible for the operation of the system shall perform the task specified herein. If the presence of the Employee may be limited during the control based on the decision of the investigating authority or the Data Owner, it may be enforced by the head of the Bank and Information Security. If during the control it may be presumed or justified that the processing of personal or sensitive data may occur, the Data Protection Officer shall also be present. In the case of a mailbox managed personally by an exiting employee, the transfer or archiving of correspondence data related to the operation of the Company and the work of the employee must be made part of the exit procedure. The work processes must be organised and carried out in such a way that the handling of working materials related to the Company's activities and the employee's work and (outgoing, incoming) communication is carried out exclusively via the receipt, registration and sending function of the central electronic business management system, and any working materials and documents issued are uploaded and attached in the system.

4.4.2. Monitoring of the use of technical devices handed over for work

Based on its legitimate interest related to workplace monitoring, the Company is entitled to monitor the use of electronic devices (such as computers, notebooks and mobile phones) handed over to Employees for work. Based on its legitimate interest related to the normal use of company devices, the Company may monitor the use and content of devices handed over to the Employees. Detailed rules concerning the use of electronic devices and mobile phones provided by the Company are included in the rules of the Information Security Regulations on the use of portable devices, which do not specify the special rules concerning personal and sensitive data, therefore, they shall be applied with the amendments specified herein.

Employees of the Bank and Information Security are entitled to perform the control in accordance with the provisions of the effective Information Security Regulation, provided that the Data Protection Officer shall be involved as approving party in the authorisation process for copying data to an external data carrier, if the copying concerns Personal and Sensitive Data.

By applying a gradual approach, the monitoring shall be primarily directed to the examination of the appropriate use of company devices. The monitoring may not result in the violation of human dignity, and the Employee's privacy may not be examined, therefore, during the monitoring, it is not possible for the Company to check contents concerning the Employee and not related to the employment relationship, or to collect, analyse and process them for such purposes even with an algorithmic solution.

During the control, the Employee shall be present, unless his or her presence would undermine the purpose of the control, or if it is impossible, or if the limitation of the Employee's rights relating to the personality is allowed for in the law. If the Employee is permanently not at his or her workplace, and his or her personally used technical devices shall be checked, the Employee may appoint another Employee. If it is clear that the subject of the files found on the device is official, then it may be handed over to the Company. If there is no appointed Employee, or he or she is not present at his or her workplace, the IT specialist who is responsible for the operation of the system and has an appropriate level of access right or is authorised shall

perform the task specified herein. If the presence of the Employee may be restricted during the control, the head of the Bank and Information Security shall inform the Data Protection Officer of the control in accordance with the decision of the Data Owner. If during the control it may be presumed or justified that the processing of personal or sensitive data may occur, the Data Protection Officer shall also be present.

For the protection of human life, physical integrity, personal freedom, performance of financial services, protection of shares, securities and assets, based on its legitimate interest related to data processing, the Company operates a CCTV camera surveillance system at its registered office. In the case of foreign representation offices, on-site digital recording of the images recorded by the cameras and remote access to the recordings shall be ensured, depending on the technical possibilities. The camera surveillance systems are operated by Bank Security employees within the framework of the Physical Security Regulations.

Recordings are stored at the place of recording and are retained for no more than sixty (60) days. The process for revision of the recordings and other circumstances of the monitoring are specified in the Physical Safety and Security Regulations.

The provisions of the Security Services Act, the Information Act and GDPR govern the keeping and use of video and audio material produced by the CCTV system.

Detailed description of the position and angle of the cameras applied by the Company are included in Schedule 2 of the Physical Safety and Security Regulations.

4.4.3. Monitoring of internet use

Based on its legitimate interest related to the workplace monitoring, the Company is entitled to monitor the internet use of Employees in accordance with the requirements of the Information Security Regulations on the use of the Internet. The monitoring may not be directed to the activities of Employees which affect their sensitive data (religious affiliation, political views, sexual orientation, etc.), not even on anonymised basis.

4.4.4. Other monitoring activities

Separate regulations may also provide for other methods for the monitoring of Employees, however, such other monitoring activities and methods shall comply with the provisions of this Regulation, and during the monitoring, a gradual and proportionate approach shall be applied in all cases, because the privacy of Employees may not be violated. In each case, the head of the organisational unit performing the monitoring and responsible for the data processing and the data processing employee of the organisational unit conducting the monitoring in question shall be liable for data processing activities carried out during such monitoring activities, as well as for their compliance with the requirements set forth in these Regulations and applicable laws.

4.5. Period of data retention

Personal data is stored at the Company only for the following time:

a) the time necessary to achieve the legitimate purpose for which the personal data is processed; or

b) the time needed to comply with the applicable legal requirement.

The Company may specify a time window (e.g. minimum duration, data storage schedule) for which data belonging to a specific category of personal data may be processed based on voluntary consent.

After the expiry of the applicable data retention period, the Data Protection Officer shall take appropriate steps to ensure that the personal data:

a) is securely erased or destroyed in accordance with relevant regulations;
b) is anonymised; or
c) is archived (if not prohibited by a legal regulation or not contrary to the applicable retention schedule).

The Data Protection Officer shall record the deadlines for erasing the different categories of data in the records of data processing activities, taking into account the relevant CEO directives.

5. Accountability and records of processing activities

In accordance with the accountability principle, the Company shall demonstrate compliance with the data protection regulations, in particular by maintaining records of processing activities in accordance with Article 30 of the GDPR. The Company shall maintain the records of processing activities, including their electronic form, in writing. The records shall contain all of the following information:

a) the name and contact details of the Company and, where applicable, the joint controller, and the Data Protection Officer;
b) the purposes of the processing;
c) the Data Subjects, and the categories of Personal Data concerned;
d) the categories of recipients to whom the personal data has been or will be disclosed, including their geographic location;
e) if the transfer of personal data is to a country that provides an inadequate level of protection or is effected on the basis of an adequacy decision, then the country that provides an inadequate level of protection or, in the case of a transfer effected on the basis of an adequacy decision, the country of destination, and, in the case of a transfer to a country that provides an inadequate level of protection, the appropriate safeguards;
f) if possible, the deadlines assigned for erasing the different categories of data; and
g) if possible, a general description of the technical and organisational measures.

The Company's records of processing activities as per Article 30 of the GDPR shall be maintained by the Data Protection Officer.

6. Data Security

The Company shall ensure the protection of Personal Data. For this, it shall implement the necessary and appropriate technical and organisational measures for Data Sets stored via electronic devices and on traditional, paper-based data carriers.

The Company shall ensure the appropriate security of Personal Data, in particular protection

against any unauthorised or unlawful processing of the data, and against the accidental loss, destruction or damage of the data.

The Company shall protect the Personal Data against unauthorised access, modification, transfer, disclosure, erasure or destruction, accidental destruction or damage, as well as its unavailability due to a change in the applied technique with measures appropriate for the requirements set forth in the IT Security Regulations and the IT Operations Regulations covering in detail the whole electronic information system.

The Company shall ensure the enforcement of the rules on Data Security by means of separate regulations, directives and procedures. To ensure that the conditions for Data Security are implemented, the Company shall provide appropriate training to the employees concerned.

The Company shall take into account the latest state of the art when defining and applying measures designed to ensure the security of Data. Of the various data processing solutions available, it shall choose the solution that ensures the highest level of protection for the Personal Data, unless this represents a disproportionate degree of difficulty or expense.

With respect to the security of Data that is not stored in electronic format, the provisions of the Company's Document Management Regulations and Physical Security Regulations shall apply.

6.1. Special rules concerning the logging, vulnerability assessment, classification of and management of access to personal data

- Logging

Logging functions and logging data of applications processing personal data and included in the central log analysing system shall be protected against unauthorised modification and access. In the case of subsystems processing personal and sensitive data, depending on the system technology solution, it shall be ensured that logging data may not generate a new system which processes personal or sensitive data.

Logging configuration may only be accessed by employees for whom it is necessary for work, and only to a limited extent. The access protection shall be established so as to ensure that the settings of the logging functions and the logged events may not be available to or modified by unauthorised persons.

The established logging system shall ensure separation, filtering and classification of log entries of personal and sensitive data.

The Information Security Regulations provide for the size limitation and ensuring the integrity of log files, taking into account the infrastructural capacities and classification of the data categories.

- Vulnerability assessment

Vulnerability assessments concerning personal and sensitive data and demonstrating compliance with the integrity requirements of the electronic information security shall be performed at least once a year, with a revision regularly performed by an independent third party. Integrity of the IT system also entails compliance with the requirements for the prevention of unauthorised access to Personal and Sensitive Data, therefore, in the absence of

an integrity criterion, an independent or targeted revision concerning Personal or Sensitive Data is necessary. If the annual regular vulnerability assessment finds that the integrity is not adequate, then a separate targeted revisions shall be performed in order to ensure that systems processing personal and sensitive data are protected. The integrity assessment or, if its not adequate, the targeted revision shall be recorded (including the drafting of a certification, an audit report, an expert summary or other status report), and in addition to the compliant elements, such records shall include all deficiencies or anomalies or risk factors which may entail unauthorised access to data or the realistic risk thereof. The findings of the revision shall be processed in an aggregated form in the annual report of the Information Security, and an action plan for the remedy of anomalies shall be prepared for the Data Owner, the system operator and, if necessary, the information security officer with the indication of the tasks, deadlines and responsible persons. The Information Security unit shall send the annual report containing the findings of the review to the Data Protection Officer for information, where affected.

- Data classification

IT systems processing Personal Data shall be classified in data classification categories taking into account other confidentiality, integrity and availability criteria. The methodology of data classification is the same as that of the Information Security Regulations for data classification. The set of requirements for the logging, access rights management and control pertaining to the data security categories is the same as the ones specified in the set of requirements pertaining to the data security categories in the Information Security Regulations.

- Access rights management, access protection

The primary purpose of managing access rights is to provide authorised users with IT and other resources and Data in the appropriate quality, continuously and uninterruptedly, by differentiating their access rights according to the extent of their work duties, while a secondary (or ancillary) purpose is to protect these from unauthorised access and misuse. General rules of access management are included in the Information Security Regulation, in the case of physical, administrative and logical protective measures ensuring the processing of personal and sensitive data, it is not justified to deviate from generally described access rights management processes and the implemented system technology solutions.

In justified cases, third parties (suppliers, partners, authorities, employees of supervisory authorities, trainees, etc.) may have access to IT system which may contain Personal Data in accordance with the authorisation set forth in their work contract, subject to the terms and limitations specified therein. Access may only be granted if it is absolutely necessary and justified for the task, it has an appropriate legal ground (agency contract or other agreement, or mandate in the case of employees of supervisory authorities or auditors, etc.), and if third persons undertake in a disclosure agreement to keep confidential data made available to them (in the case of legal persons or entities with the disclosure agreement signed by natural persons who take part in the performance of the contract). The obligation to sign the disclosure agreement shall be set forth in the contract.

Should any question occur when granting access to external contractual parties to IT systems which contain personal data, the Data Protection Officer shall be consulted. Natural persons who have signed a disclosure agreement may not have access to Personal and Sensitive Data

processed in the IT system.

The limit values for the physical environment of server and engine rooms performing the processing of personal data are the same as the ones set forth in the physical parameters of the Information Security Regulations for data centres. The employee or expert appointed for the management of the network shall inform the Data Protection Officer according to paragraph 7 of any changes negatively affecting personal data categories (breach).

7. Personal data breach

All Employees shall report to their direct supervisor as well as to the Data Protection Officer (Schedule 3 of these Regulations) – where possible, in writing – should they become aware of the occurrence of an incident endangering Data Security or of a personal data breach, or of the possibility of the occurrence of such, immediately after having become aware of such.

A third party may report a Personal Data Breach related to the Data processed by the Company or the Processor acting on its behalf to the email address exim@exim.hu accessible on the Company's website.

The Data Protection Officer shall examine the reported personal data breach within twenty-four (24) hours in order to determine whether risk exists that the Data Subjects may not enforce their rights. If this is not likely, then he or she assesses the report in terms of whether it is necessary to notify another organisational unit regarding the report concerned. If based on the report it is justified to involve other organisational units, then he or she shall transfer the report to the head of the unit in question within twenty-four (24) hours.

If, as a result of the investigation, it transpires that there is a risk that the rights of the Data Subject may be violated, he or she shall report the personal data breach the Authority as soon as possible, but certainly no later than 72 (seventy-two) hours after he or she becomes aware of the personal data breach.

In the report to the Authority, the Data Protection Officer shall:

- the content of the Personal Data Breach, including the scope of the Data Subjects and the scope of the Data affected by the breach,
- provide information on the name and contact details of the Data Protection Officer or other contact person designated for providing further information,
- 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.

The Data Protection Officer shall maintain records on personal data breaches (Schedule 4 of this Regulation). Retention period for the records and the minutes made of the personal data breach: ten (10) years. The Data Protection Officer shall ensure that entries older than 10 years are deleted. The records relating to Personal Data Breaches shall contain the following information:

- Scope of data affected by the personal data breach;
- Scope of persons affected by the personal data breach;

- Date of the personal data breach;
- Circumstances of the personal data breach;
- Impacts of the personal data breach;
- The measures taken;
- Other data.

If the Personal Data Breach is likely to have consequences that significantly affect the exercise of a fundamental right of the Data Subject (high-risk personal data breach), the Company shall inform the Data Subject of the Personal Data Breach without delay.

The Company shall not inform the Data Subject if:

- prior to the Personal Data Breach, the Company applied appropriate technical and organisational protection measures in respect of the Data involved in the Personal Data Breach – in particular, measures rendering the Data incomprehensible in the event of unauthorised access or resulting in their encryption – and if necessary, the Data Protection Officer may request an opinion on the appropriateness of such measures from the head of IT Operation.
- measures taken after its becoming aware of the personal data breach ensure that the consequences of the personal data breach that would otherwise have significantly affected the exercise of a fundamental right of the Data Subject are no longer likely to occur. If necessary, the Data Protection Officer shall provide a written statement on this.
- directly informing the Data Subject could only be achieved with a disproportionate effort, and therefore it provides the Data Subjects with adequate information related to the personal data breach through information published in a way that is accessible to anyone (e.g. via the internet). The Data Protection Officer shall decide whether this method of information provision should be used.

8. Processor

In the course of its activities, the Company may use a Processor on a permanent or ad hoc basis. Processors may be engaged on a permanent basis primarily if this is necessary for the performance of administrative tasks arising from the services related to the activities of the Company or for the maintenance of the IT system. With respect to use of the Processor, the legal regulations relating to data protection, in particular the provisions of the GDPR, shall apply. The use of a Processor may only take place on the basis of a written contract, which must specify the tasks that need to be performed in relation to Data Protection and Data Security. A sample document of the contract to be concluded with the Processor is available in Schedule 8 of these Regulations.

The Company shall specify the rights and obligations of the Processor related to the processing of Personal Data in accordance with the relevant legal regulations on data protection. The Company shall be responsible for the lawfulness of the directives relating to data processing operations.

If in accordance with the contract concluded with the processor personal data are processed, then the contract may only be concluded if the natural persons involved in the processing (including co-operators, subcontractors, agents, experts, consultants and employees acting on behalf of the contractual partner) as data processors sign a disclosure agreement with the Company, and undertake to comply with the requirements under Article 28 of the GDPR, and to provide the Company with the possibility to check such compliance. The declaration must

be made in the contract relating to Data Processing set out in Schedule 8 to these Regulations and must be kept together with the relevant contractor's agreement or assignment contract (Underlying Contract).

Within the scope of activities of the Processor and the framework specified by the Company, the Processor is liable for the processing, modification, erasure, transfer and disclosure of personal data. During performance of its activities, the Processor may use the services of another Processor only in accordance with the instructions of the Company.

The Processor may not make substantive decisions related to data processing, may process the personal data made available to it only in accordance with the instructions of the Company, may not perform data processing for its own purposes, and must store and retain personal data in accordance with the instructions of the Company.

By concluding the contract included in Schedule 8, the Company ensures that the rights of the Data Subjects may not be violated during the activities of the Processor, and that the Processor may only access Personal Data if it is indispensable for the performance of its duties.

The Company may entrust data processing only to a person or organisation that provides adequate safeguards for the implementation of technical and organisational measures suitable for ensuring the lawfulness of the data processing and for protecting the rights of the Data Subjects.

In order to provide evidence of these safeguards, according to the rules of the data protection impact assessment, the Processor must fill in the questionnaire prepared by the Data Protection Officer for the data controller before starting the data processing. (Data Protection Risk Assessment)

The Processor explicitly undertakes in the contract to be concluded with the Company that the data processing will comply with the requirements of the GDPR. The contract between the Company and the Processor, as set out in Schedule 8, shall, in accordance with Article 28 of the GDPR, specify at least the following:

a) A statement by the Processor that it has the technical and organisational conditions required to protect the rights of Data Subjects in accordance with the Regulation;
b) The Processor may not use an additional data processor (sub-processor) without the prior written ad hoc or general authorisation of the Company;
c) The object, duration, nature and purpose of the data processing performed by the Processor, the type of personal data, and the categories of the Data Subjects;
d) The Processor's consent to the processing of personal data only on the basis of the Company's written instructions, including the transfer of personal data to a third country or international organisation, unless the processing is required by EU or Member State law applicable to the performer of the outsourced activity;
e) The Processor shall assist the Company in responding to requests for the exercising of Data Subjects' rights;
f) In a separate clause, the Processor shall undertake to treat personal data confidentially and to comply with the data security measures required by the GDPR;
g) The Processor's commitment to delete or return all personal data to the Company and delete existing copies at the discretion of the Company upon termination of the provision of the data processing service, unless EU or Member State law requires the storage of the personal data;
h) The Processor's commitment to ensuring that persons authorised to process personal data

undertake a commitment to confidentiality or are subject to a legal obligation to maintain confidentiality.

The Processor shall keep records of its data processing activities carried out on behalf of the Company in accordance with Article 30 of the GDPR and shall immediately notify the Company in all cases where it becomes aware of a breach of the rules on the processing of personal data.

It shall provide the Company with all the information necessary for evidencing the fulfilment of the obligations set out in the GDPR.

The Company shall provide the Data Subject with information on the identity of the Data Processors used by it before the start of the Data Processing or at the subsequent request of the Data Subject. The Company shall comply with this information provision obligation by publishing a notice in accordance with Article 13 of the GDPR on the Company's website within 5 (five) working days after the signing of the contract concluded with the Processor. The publication of the notice shall be initiated by the organisational unit responsible for concluding the contract by contacting the Data Protection Officer, who shall prepare the notice immediately after concluding the contract and send it to the Marketing department within 3 (three) working days. The Data Protection Officer shall keep the details of the Processors (name, registered office address) in the electronic data protection register maintained by him or her. Details of the Processors in the data protection register maintained by him or her

Within five (5) working days after the signing of the contract concluded with the Processor, and based on the initiative of the Data Protection Officer, the Company shall publish the name and contact details of the Processor, the contact details of the Company's Data Protection Officer, the purpose of the planned processing and the Data Subject's rights, as well as the means to exercise them.

9. Outsourcing

The Company may outsource any activities related to its financial and ancillary financial service activities, or such activities as it is required to perform by law, that involve Data Management, Data Processing or data storage, subject to compliance with the data protection regulations. It shall hand over data necessary for or related to the performance of the outsourced activity to the person performing the outsourced activity.

During selection of the person performing the outsourced activity, preparation and conclusion of the outsourcing agreement, and monitoring of the performance of the outsourced activity, the Company shall ensure that Personal Data is protected at the person performing the outsourced activity.

Rules specified in Section 8 shall apply to the person performing the outsourced activity.

The Bank shall provide information on the outsourced activity and the persons performing such activity on its website (www.exim.hu) and in the Business Regulations.

10. Data transfer

A request for disclosure of information with respect to personal data from outside the Company,

from a third party, shall, in the absence of a statutory provision on the matter, only be fulfilled by the Company if the Data Subject authorises the Company in this regard in writing. The Data Subject may also grant such authorisation in advance, which may apply to a certain period, purpose and specified range of entities that may request the data. The authorisation shall be kept by the Data Protection Officer for the duration of Data Processing and for 10 (ten) years from the termination thereof, and he or she shall ensure that the Data is communicated.

Regardless of the Data Subject's declaration of consent, requests based on legal authority from third parties from the criminal authorities (police, courts, prosecutor's office), the National Tax and Customs Administration and the national security services must be complied with. The head of the organisational unit that fulfils the request shall promptly inform the CEO and the Data Protection Officer of the requests from these organisations on the next working day after the receipt of the request, by electronic means. Based on the written opinion of the Data Protection Officer, the provision of the data affecting personal data may be performed subject to notifying the CEO at the same time. The CEO may lodge a complaint of non-suspensory effect with the competent minister against the request of the national security services for data provision.

The relevant organisational unit shall prepare a report on the personal Data Transfers to a Third Party, and shall send it to the Data Protection Officer within 1 (one) working day after the data transfer has taken place. The Company's records of processing activities under Article 30 of the GDPR shall contain the data transfers.

Before personal data transfers to third parties, the Data Protection Officer shall examine the accuracy, integrity and up-to-dateness of the data.

10.1. Data transfer abroad

In the case of certain instances of data processing, the Company may transfer personal data to a third country outside the European Economic Area or to an international organisation ("**Transfer of Data Abroad**"). Personal Data Transfers abroad shall always be approved by the Data Protection Officer, and his or her approval shall be recorded in the Request form.

The Transfer of Data Abroad may only take place if the European Commission ("**Commission"**) has established that the third country provides an adequate level of protection with respect to personal data ("**Adequacy Decision"**).[2]

In the absence of the Adequacy Decision, the Company may only transfer personal data if the recipient controller or processor has provided adequate safeguards with respect to the processing. Such safeguards may include, without the express permission of the competent supervisory authority:

- general data protection clauses adopted by the Commission or general data protection clauses adopted by the supervisory authority and approved by the Commission;
- an approved code of conduct together with a binding and enforceable commitment from the third country controller or processor to apply – including with respect to the rights of

[2] Andorra, Argentina, Faroe Islands, Guernsey, Israel, Jersey, Canada, Isle of Man, Switzerland, Uruguay, USA, New Zealand

Data Subjects – the appropriate safeguards;
- an approved certification mechanism together with a binding and enforceable commitment from the third country controller or processor to apply the appropriate safeguards, including with respect to the rights of Data Subjects.

In the absence of adequate safeguards, the data transfer may take place if one of the following conditions are met:

- the Data Subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of the transfer due to the absence of an adequacy decision and appropriate safeguards;
- the transfer is necessary for the performance of a contract between the Data Subject and the controller or the implementation of pre-contract measures taken at the Data Subject's request;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between the controller and another natural or juridical person;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise or defence of legal claims;
- the transfer is necessary in order to protect the vital interests of the Data Subject or of other persons, and the Data Subject is physically or legally incapable of giving consent;
- the transferred data comes from a register that according to Union or Member State law is intended to provide information to the public and that is open to inspection either by the public in general or by any person who can demonstrate a legitimate interest in it, but only if the conditions laid down by Union or Member State law for inspection are met in the particular case.

If the transfer cannot be based on adequacy, there are no adequate safeguards in place, and none of the derogations for special situations apply, the transfer to a third country can only take place if:

- the data transfer is not of a repeating nature,
- it concerns only a limited number of Data Subjects,
- it is necessary for the pursuit of a compelling legitimate interest of the controller such that are not overridden by the interests or rights and freedoms of the Data Subject, and
- the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of the personal data.

In such cases, the Data Protection Officer shall immediately inform the supervisory authority of the transfer, and beyond fulfilling the general information-provision obligations, he or she shall inform the Data Subject of the transfer and of the controller's compelling legitimate interest pursued.

11. Providing information to the Data Subjects

The Company shall ensure that the Data Subjects are provided with adequate information on the purpose of the processing of the personal data, and upon request, provide all other information that concerns the data processing activities related to the Data Subjects.

The Company is obliged to provide the Data Subjects with the details of the processing of their

personal data mentioned in Articles 13 and 14 of the GDPR in the form of appropriate data processing notices according to Schedule 7. Information shall be provided to Data Subjects in a concise, transparent, comprehensible and easily accessible form, and in a clear and comprehensible manner.

The Data Protection Officer shall be responsible for the drafting of the notices.

11.1. Providing information if the personal data has been collected from the Data Subject

The Company shall inform the Data Subject of the following:

a) the primary and secondary purposes for which the personal data is processed and the related legitimate interest of the Company, if any;
b) the name and contact details of the person responsible for data processing at the Company;
c) the nature and categories of the processed personal data;
d) the categories of the employees of the Company and third persons to whom personal data is transferred (if any);
e) how the Data Subjects' rights are exercised, including information on the right to lodge a complaint with the Authority;
f) if the Company intends to transfer personal data to a country that does not provide an adequate level of protection, or on the basis of an adequacy decision, then information on the appropriate safeguards, as well as on how to obtain a copy of these or on how to access them for perusal;
g) the period for which the personal data will be stored or, if that is not possible, the criteria for determining that period;
h) the contact details of the Data Protection Officer;
i) whether the provision of personal data is a statutory or contractual requirement, or a precondition for concluding a contract, and the consequences of failure to provide such data.

11.2. Providing information if the personal data has not been collected from the Data Subject

If the personal data has not been collected directly from the Data Subject, the Company shall inform the Data Subject of the following:

a) the information specified in Section 11.1;
b) the (publicly available) source of the personal data;
c) this information must be provided:
   - at the time of recording the personal data in a database of the Company, but no later than within one month after the personal data is obtained; or
   - if the personal data is communicated to other recipients, at the latest when the personal data is communicated to the other recipients for the first time.

11.3. Exceptions

The provisions of Section 11.2 shall not apply if

a) if providing the information to the data subject is impossible or would involve disproportionate effort; or

b) would involve disproportionate costs; or
c) the obtaining or disclosure of the Data is expressly required by an instrument of law applicable to the Company, which requires appropriate measures to be taken to protect the legitimate interests of the Data Subjects.

In all cases it is the Data Protection Officer who decides whether the above exceptions apply.

12. Rights of the Data Subject, enforcement of the rights

Data Subjects whose personal data are processed by the Company as controller based on their voluntary consent shall have the following right in accordance with this Regulation:

- right to access;
- right to rectification;
- right to erasure;
- Right to restriction of processing;
- right to data portability;
- right to object.

The procedural rules related to the rights of the Data Subject are set out in Section 12.7 of these Regulations.

12.1. Right to access

Each Data Subject is entitled to receive feedback on the processing of data processed by or on behalf of the Company, which feedback shall include:

a) the legitimate purposes of the processing;
b) the categories of Personal Data concerned;
c) the categories of the recipients of the personal data concerned;
d) if possible, the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
e) the source of the personal data, if the personal data is not collected from the Data Subject;
f) if the personal data is transferred to countries that do not provide an adequate level of protection or if the transfer is based on an adequacy decision, the appropriate safeguards.

In addition to the feedback, the Company – at the request of the Data Subject – provide the Data Subject with the following information:

a) information on the Data Subject's right to request the rectification or erasure of his or her personal data at any time, as well as on his or her right to request the restriction of the processing of his or her personal data and the right to object to the processing of his or her personal data;
b) the possibility of submitting a complaint to the Authority; and
c) the possibility of judicial redress; and
d) where relevant, the possibility of claiming compensation for breaches of binding corporate regulations.

In order to enforce the right of access, the Company shall inform the Data Subject, at his or her request, whether his or her personal data is processed by the Company or by a data processor acting on its behalf or at its instruction.

12.2. Right to rectification

The Data Subject shall be entitled to request rectification of inaccurate data concerning him or her. Subject to the purpose of the data processing, the Data Subject is entitled to request – through a supplementary statement, among other means – the supplementation of incomplete personal data concerning him or her.

12.3. Right to erasure

The Data Subject shall be entitled to request erasure of personal data concerning him or her if

a) The personal data is no longer necessary in relation to the legitimate purposes for which they were collected or otherwise processed;
b) the Data Subject withdraws his or her consent, and the data processing has no other legitimate purpose;
c) the Data Subject successfully objects to processing of his or her personal data pursuant to Section 12.6;
d) the personal data of the Data Subject has been unlawfully processed; or
e) the personal data of the Data Subject must be erased in order to fulfil a legal obligation.

12.4. Right to restriction of processing

The Data Subject shall be entitled to request the restriction of the processing of personal data concerning him or her if

a) the accuracy of the Personal Data is contested by the Data Subject, for a period enabling the Company to verify the accuracy of the Personal Data;
b) the Processing is unlawful;
c) the Company no longer needs the Data for any legitimate purpose, but the Data Subject requires it for the establishment, exercise or defence of legal claims; or
d) the Data Subject has objected to the processing of his or her personal data as per Section 12.6, until the existence of the legitimate interest of the Company is established.

Any restriction on the processing of the Data Subject's personal data may affect the services provided by the Company.

During the restriction of data processing, the personal data may be processed, with the exception of storing it, only with the consent of the Data Subject, or for the establishment, exercise or defence of legal claims, or for the defence of the rights of another natural or juridical person.

The Company must notify the Data Subject before lifting the restriction on data processing.

12.5. 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 the Company, in a structured, commonly used and machine-readable format, where:

a) processing is based on the Data Subject's consent; or
b) the processing is based on the performance of a contract concluded with the Data Subject; and the processing is carried out by automated means.

12.6. Right to object

The Data Subject shall have the right to object, on grounds relating to his or her particular situation, at any time to the processing of his or her personal data carried out in the public interest or in the exercise of the public authority vested in the Company or that is necessary for the enforcement of a legitimate interest of the Company or of a third person.

Furthermore, the Data Subject shall have the right to object to the processing of his or her personal data based on legitimate interest, if the Company can demonstrate that the processing is necessary for the purposes of compelling legitimate interests which provide legitimate ground for the processing or which relate to the enforcement or protection of legal claims.

12.7. Provisions related to the exercise of the Data Subject's rights

The written request of the Data Subject, received in paper format, shall be filed in accordance with the provisions of the latest effective Document Management Regulations, after which the organisational unit responsible for filing shall forward the request to the Data Protection Officer without delay, but certainly no later than on the working day following the filing. Requests for the exercise of Data Subjects' rights received electronically at info@exim.hu shall be forwarded by the Marketing department within one (1) working day to the Data Protection Officer.

Before examining the obligation to comply with the request, the Data Protection Officer shall, if the request is incomplete, ask the Data Subject for:

a) a definition of the type of personal data to which he or she wishes to have access;
b) a definition of the circumstances in which the Company has collected the data;
c) satisfactory proof of his or her identity; and
d) in the case of a request for rectification, erasure, restriction or objection, a statement of the reasons why the personal data is inaccurate, incomplete or not processed in accordance with the relevant legal provisions or these Regulations.

Within one (1) month of receipt of the request, the Data Protection Officer or the person responsible for maintaining contact with the Data Subject shall inform the Data Subject in writing:

a) of the Company's decision with respect to the submitted request and measures taken or planned in response to the request;
b) if additional information or clarification is required in order to continue to deal with the request effectively; or
c) the deadline extension and the final deadline when the Company will notify the Data Subject of its position, which may not be later than two months from the receipt of the request.

The Data Protection Officer shall prepare a draft letter of response, if necessary with the involvement of Legal Services and the organisational unit performing the Data Processing. In the case of the involvement of Legal Services and the relevant organisational, at least 3 (three) working days must be provided for Legal Services and the unit concerned.

If the Company does not take action at the request of the Data Subject, it shall inform the Data Subject of the following without delay, but no later than within 1 (one) month from the receipt of the request:

a) the reason for not taking action;
b) the possibility of submitting a complaint to the Authority; and

c) the possibility of judicial redress.

The Data Protection Officer shall register the requests received by the Company electronically in his or her own organisational folder.

If, at the request of the Data Subject, it is necessary to provide information or take action, the Data Protection Officer shall immediately inform the department concerned of the need to do so.

The Company shall provide information and measures following the exercise of Data Subjects' rights for free. If the request is unfounded, or excessive in scope or in terms of its repetitive nature, the Company shall, based on the opinion of the Data Protection Officer, be entitled to charge a reasonable administrative fee for providing the requested information or for taking action, or may refuse to provide the requested information or take action.

The amount of the cost reimbursement shall be determined by the head of Accounting based on the costs specified in Schedule 2 of these Regulations, and the Company shall inform the Data Subject of the amount of this in advance. The Data Subject shall decide within thirty (30) days after receipt of the notice on the reimbursement whether he or she wishes to maintain his or her request for information. If the Data Subject maintains his or her request, he or she shall pay the amount of the reimbursement to the Company within the deadline indicated on the invoice issued by the Company, by bank transfer to the bank account number indicated on the invoice.

If the data request entails the reimbursement of costs, the Data Protection Officer shall request information on the amount of these costs electronically from Accounting within three (3) working days. Accounting shall inform the Data Protection Officer of the cost of the data request within one (1) working day, and the Data Protection Officer shall send the prior information on the amount of the reimbursement to the Data Subject in writing within three (3) working days. The Company shall provide the information requested by the Data Subject after reimbursement of the costs in accordance with the above. Any reimbursement of costs already paid shall be refunded by the Company if the Personal Data has been processed unlawfully by the Company or a request for information has led to rectification.

In each case, the Chief Executive Officer shall decide whether to provide information, take action or to refuse the above, taking into account the views of the Data Protection Officer and the head of Legal Services.

12.8. Judicial remedy

If the Company does not deal with the Data Subject's request for the exercise of his or her rights related to the processing of personal data, or does not provide a response regarding the procedural actions taken in relation to the request, or on the results of these actions, within 3 (three) months, or if the Data Subject otherwise believes that the processing of his or her personal data by the Company violates his or her rights under the GDPR, he or she may turn to the court with jurisdiction in the location of the Company's registered office or in the location of the Data Subject's home address.

12.9. Compensation, indemnification

A Data Subject, or any other person, who has suffered pecuniary or non-pecuniary losses as a result of a breach of the data protection and data security provisions of these Regulations or of the stipulations of the GDPR may claim compensation and aggravated damages from the

Company or from a Processor performing data processing activities on behalf of the Company under a contract.

The Company shall be liable to the Data Subject for any losses caused by the Data Processor used by it and the Company shall also pay to the Data Subject aggravated damages in the event of an infringement of personality rights caused by the Processor.

The Company may be released from the obligation to pay compensation and aggravated damages in the cases specified in Article 82 of the GDPR.

13. Disclosure of Personal Data

Disclosure of Personal Data processed by the organisational units of the Company is prohibited unless authorised by the Data Subject or required by law. Aggregate statistical data related to the Company's Employees, Suppliers, Supported Parties and Clients – even if based on Personal Data – may be disclosed provided the Data Subject cannot be identified from them. Prior to the disclosure of the Personal Data, the Company's Employee is obliged to make sure that it is not possible to identify the Data Subject on the basis of the provided Personal Data. In case of doubt, the Data Protection Officer shall be consulted in writing.

14. Performance of interest assessment tests

Personal data may be processed even if it is impossible to obtain the data subject's consent or if this would incur excessive cost, or if the Data Subject has withdrawn his or her consent, and the processing of personal data is necessary for compliance with a legal obligation to which the Company is subject, or if it is necessary for the enforcement of the legitimate interests of the controller or a third person, and the enforcement of such legitimate interest is proportionate to the restriction of the Data Subject's rights related to the protection of his or her personal data. This means that the interests of the Company or third person are "stronger" than the Data Subject's right to the protection of his or her personal data, which shall be determined by the Company during performance of an interest assessment test involving a comparison of these rights. The interest assessment test shall be carried out by the Data Protection Officer based on consultation with the organisational unit which carries out the processing within three (3) working days, the result of which shall be communicated to the Data Subject and the organisational unit carrying out the processing by the Data Protection Officer.

15. Data Protection Controls

Compliance with data protection procedures and in particular the provisions of this Regulation shall be regularly checked by the heads of organisational units involved in the Processing.

The Data Protection Officer shall ensure compliance with statutory rules of Processing by reviewing regulations, records and registers related to document management and data processing.

The Data Protection Officer shall initiate and conduct monitoring of the compliance of processes related to personal data processing with the provisions of legal regulations on data protection and this Regulation. Subject to the CEO's approval, the Data Protection Officer may engage an external expert for examination of the adequacy of the level of data protection. The

Data Protection Officer shall prepare a schedule for the data protection controls planned for the given calendar year. Methodology of controls shall be established by the Data Protection Officer.

The Data Protection Officer shall prepare the schedule for controls for the next calendar year on or before 31 December and shall report to the CEO both orally and in writing the results of data protection controls on or before 31 March of the following year, and shall inform the Board of Directors and the Supervisory Board of his or her work performed during the previous year at the first meeting after acceptance of the report.

Based on the written report made related the experiences and recommendations of the control, if a violation has occurred or is suspected, the CEO shall call the Employee involved in the Processing for its termination and/or the head of the organisational unit responsible for the process involved in the Processing. If an Employee breaches this Regulation, it shall be considered a serious breach of his or her employment contract, which may result in an adverse legal effect against the Employee or the immediate termination of his or her employment. If a person who is not an employee of the Company breaches this Regulation, it may serve as a basis for termination of the Contract concluded with him or her by the Company.

The Data Protection Officer shall keep the records of data protection controls approved by the CEO for ten (10) years from the date on which they were created.

16. Data protection trainings

The Data Protection Officer shall provide the Data Subjects with training on data protection in the following cases:

- for new Employees after their admission within the framework of a joint e-learning programme organised on a quarterly basis, but no later than at the end of the year;
- in the case of changes in data protection tasks and responsibilities (such as organisational change, operative change);
- if there is a data protection threat or incident;
- in all cases where the head of the organisational unit initiates it.

The Data Protection Officer shall define the scope of persons involved in the training and the topics to be discussed.

The Data Protection Officer shall keep the attendance records of the e-learning training stored by the training program for 10 (ten) years.

17. Publication of and access to data of public interest and data made public on the grounds of public interest

In accordance with the provisions of the Freedom of Information Act and other legal regulations related to the enforcement of the basic right to access data of public interest or data made public on the grounds of public interest (hereinafter: Freedom of Information), the Company shall ensure access to data of public interest and data made public on the grounds of public interest within the limitations set forth by the law.

Enforcement of the Freedom of Information shall be ensured by the Company through separate regulations, directives and rules of procedure.

18. Closing provisions

These regulations shall enter into force on the day following their publication, superseding the Bank's CEO Directive No. 73/2020 on the data protection and data security regulations, and Insurer's CEO Directive 65/2020.

Person responsible for reviewing the regulations: Data Protection Officer.

The Data Protection Officer shall review these Regulations in the event of every organisational, operative and legal change, but at least on an annual basis, and, if necessary, shall initiate its modification.

Budapest, 16 March 2022

Gergely Jákli (signed by)
Chairman & CEO

Schedules:

Schedule 1: Data of the Data Protection Officer
Schedule 2: Registration form and expense form
Schedule 3: Reporting sheet – In the case of personal data breach
Schedule 4: Records of personal data breaches
Schedule 5 Data processing notice for Employees
Schedule 6: Privacy policy statement
Schedule 7: Data protection notice for Clients
Schedule 8: Data Processing Contract Template