Data Protection and Data Security Regulations

1. Purpose and scope 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 Hungarian Magyar Export-Import Bank Ltd. (hereinafter: 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: Privacy 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 or GDPR).

Scope of the Regulation

The material scope of these Regulations extends to all personal data and to all Data Management and Data Processing involving the Personal Data of natural persons carried out at the Company – at its head offices, permanent establishments 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 extends to all senior officers of the Company, to the chairperson and members of its Supervisory Board and its Board of Directors, to its employees, and to persons employed under any other legal arrangement for the conduct of work, as well as to 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).

With respect to the processing of data related to money laundering, the provisions of the latest version of the CEO Directive on the prevention and combating of money laundering and terrorist financing shall apply.

If an item of data is classed as classified data or as data related to money laundering, or as protected data (a business and/or banking secret), the stricter data protection provisions must be applied. If there is any doubt as to which provisions of these Regulations should be applied to an item of data, the opinion of the Data Protection Officer shall be definitive in the matter.

The provisions set out in these Regulations shall become applicable from the day the Regulations are published.

1.2. 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 (Hungarian Standard MSZ ISO 2382-1).

Data set: the totality of Data processed in a filing system.

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.

Health data: personal data relating to the physical or mental health of a natural person, including data relating to health services provided to a natural person which contain information on the state of the natural person's health.

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.

Public interest data: based on Section 3 (5) of the Privacy Act, information or data other than personal data, registered in any mode or form, controlled by the Company concerning its activities or generated in the course of performing its public tasks, irrespective of the method or format in which it is recorded, 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 Privacy Act, all Data which does not fall within the concept of Public Interest Data, the disclosure, acquaintance or making available of which is required by law in the public interest. In accordance with Section 26 (2) of the Privacy Act, the name of the person undertaking tasks within the scope of responsibilities, as well as their scope of responsibilities, scope of work, executive mandate and other personal data relevant to the

provision of their 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 Privacy 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 means all data falling in the special categories of personal data that are personal data revealing racial or ethnic origin, political opinion, religious belief or worldview, or trade union membership, as well as genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Personal Data: any information relating to an identified or identifiable Data Subject; a natural person is identifiable if he or she can be identified, in a direct or indirect manner, on the basis, especially, of an identifier such as a name, number, place-determining data, or online identifier, or on the basis of one or more factors relating to the natural person's physical, physiological, genetic, intellectual, economic, cultural or social identity.

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: the foreign or domestic business organisation or sole trader to whom (to which) the Company provides a financial, ancillary financial or investment service within its scope of activity, as well as the business organisation or natural person that provides collateral securing a claim arising from the financial, ancillary financial or investment service for the benefit of the Company. The supplier and the supported party shall also be a client.A supplier is a natural person or business organisation that have or wish to have a contractual relationship with the Company for the selling of goods or provision of services. Sponsored Parties are natural persons, business entities, organisations, associations, foundations to which the Company provides or plans to provide grant upon request or based on its own decision for free; as well as beneficiaries from whom the Company expects to present this sponsoring activity in exchange for the support, or with whom the Company plans to conclude a contract for this purpose.

TERMS CONCERNING RESPONSIBILITIES RELATED TO DATA PROCESSING

‘**Controller**’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. For data processing activities performed in accordance with this Regulation, the Company shall be the Controller.

‘**Processor**’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

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

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

‘**Authority**’ means the National Data Protection and Freedom of Information Authority.

‘**Unauthorised person**’ means those who are not entitled to consult the Data.

National Bank of Hungary: hereinafter MNB.

TERMS RELATED TO THE PROCESSING OF DATA

‘**Data processing**’ or ‘**processing**’ means any operation or set of operations that is performed on data, regardless of the procedure applied; in particular collecting, recording, registering, organising, storing, modifying, using, retrieving, transferring, disclosing, synchronising or connecting, blocking, erasing and destroying the data, as well as preventing their further use. Taking photos and making audio or visual recordings, as well as registering physical characteristics suitable for personal identification (such as fingerprints or palm prints, DNA samples and iris scans).

‘**Restriction of processing**’ means the marking of stored personal data with the aim of limiting their processing in the future.

‘**Data destruction**’ means the complete physical destruction of the data medium that contains the data.

‘**Data transfer**’ means providing access to the data for a designated third party.

‘**Data erasure**’ means making the data unrecognisable in such a way that its restoration is no longer possible.

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

‘**Original purpose**’ means the purpose for which personal data were collected.

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

‘**Legitimate interest**’ means the legitimate (business) interest of the Company or a third person which overrules the basic rights and freedoms of the Data Subject(s), and shall apply when data processing is carried our 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**’ means the definition of the purposes and means of data processing by two or more controllers.

‘**Onward data transfer**’ means the transfer of personal data, by way of transfer to a controller or processor engaged in data processing in any third country or in the framework of an international organisation, to a controller or processor engaged in data processing in any other third country or in the framework of an international organisation.

‘**Disclosure**’ means making the data accessible to anyone.

‘**Profiling**’ means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a data subject, 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.

DATA SECURITY DEFINITIONS

‘**Personal data breach**’ means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed, especially unauthorised disclosure, modification, transfer, disclosure, erasure or destruction, as well as accidental loss or damage. (such as physical or virtual break-in, Data Processing without authorisation, unauthorised access).

‘**Security**’ means that 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)**’ means any operation or event, or the lack of such operation or event which may endanger protection or Security.

1.3. Data types

The following types of data defined in legal regulations may occur at the Company:

- Personal data (including data concerning people acting on behalf of Clients, Suppliers and Sponsored Parties, as well as Employees and data specified in property declarations),

- business secret,
- bank secret.

2. Regulations relating to data protection

2.1. Legislative background

Legislation pertaining to data protection:

- 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 (hereinafter: "General Data Protection Regulation" or "GDPR")
- Act CXII of 2011 on Informational Self-Determination and Freedom of Information (hereinafter: "Privacy Act");
- Act CXXII of 2011 on the central credit information system;
- ACT XLII of 1994 on the Hungarian Export-Import Bank Corporation and the Hungarian Export Credit Insurance Corporation(„Etv.");
- Government Decree 85/1998 (V.6.) on the Interest Equalisation System of Hungarian Export-Import Bank Limited;
- PM Decree 16/1998 (V.20.) on the detailed rules on settlement with the central budget by the Hungarian Export-Import Bank Rt. and Hungarian Export Credit Insurance Rt.;
- Decree No 50/2016. (XII. 12.) of the Governor of the Magyar Nemzeti Bank on the reporting obligations for the central bank information system to be fulfilled primarily in the relation to carry out the basic tasks of the Magyar Nemzeti Bank
- Act CCXXXVII of 2013 on Credit Institutions and Financial Enterprises ('Act on Credit Institutions');
- Act CXCV of 2011 on Public Finance (hereinafter: 'Public Finance Act');
- Act CXXXIX of 2013 on the National Bank of Hungary;
- Act LIII of 2017 on the Prevention of Money Laundering and Terrorist Financing;
- Act V of 2013 on the Civil Code of Hungary ("Ptk.");
- Act I of 2012 on the Labour Code ('Labour Code');
- Act LXXX of 1997 on the Eligibility for Social Security Benefits and Private Pensions and the Funding for These Services ('Tbj.');
- Act CXVII of 1995 on Personal Income Tax ('Act on Personal Income Tax');
- Government Decree No. 451/2016 (XII.19.) on detailed rules regarding the operation of the electronic public procurement system;
- GKM Decree No. 114/2007 (XII.29.) on the rules of digital archiving;
- Act XLVI of 1993 on Statistics;
- Act CLII of 2007 on the obligations of submitting declaration of assets and liabilities;
- Recommendation 5/2016 (VI. 06.) of the National Bank of Hungary on the establishment and operation of internal defense lines and the governance and control functions of financial organizations.

3. Data processed by the Company

3.1. Principles of Data Processing

The Company as Data Controller shall be responsible for, and be able to demonstrate compliance with data protection rules.

With respect to Data Processing Activities, the Company shall act in accordance with the requirements of good faith, fairness and transparency, in cooperation with Data Subjects. The Company shall exercise its rights and obligations related to Data Processing for the purposes intended, lawfully and in a transparent manner in relation to the data subject.

During Data Processing Activities, the Company shall ensure accuracy, integrity and up-to-dateness of the Data, if necessary for the purpose of the Data Processing, and that the identification of data subjects is permitted for no longer than is necessary for the purposes for which the personal data are processed. Furthermore, it shall take every reasonable step to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

Personal data may be collected, stored, processed and transferred for specified, explicit and legitimate purposes, and may not be further processed in a manner that is incompatible with the original purposes. The Company shall regularly examine the purposes and means of data processing in order to ensure that they are adequate, relevant, necessary and proportionate. The Company shall adequately document this activity.

The Company shall store Personal Data in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or 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 unauthorized or unlawful processing of data, accidental loss, destruction or damage.

The Company shall process personal data in a manner that ensures the availability of rights for Data Subjects, as well as the integrity and confidentiality of data.

The Company shall not apply decision-making or profiling based on automated processing.

3.2. 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) **in order to ensure responsible, effective and efficient business management, with special respect to the following activities**:
   i. for the pre-contractual evaluation of clients, performance of the contract concluded or to be concluded with the client, suppliers or sponsored parties, performance of financial transactions, and contact with clients and other contractual partners, as well as compliance with requests for further information submitted by clients, Data Subjects, suppliers or sponsored parties or exercise of their legal claims;
   ii. for the maintenance of business and client relationship, systematic management of user names and passwords, as well as maintenance and extension of contacts with clients, suppliers and sponsored parties, for statistical and scientific purposes;
   iii. for the implementation of business processes, organisational and asset management, performance of internal controls and assessments, performance of financial and accounting tasks, management of executive summaries and assessments;
   iv. for safety and especially property protection, as well as for identification of Data Subjects, clients or suppliers and determination of their access rights;
   v. for performance of the legitimate interests of the Company or any other third person;
   vi. for the performance of legal obligations.

b) **for supporting activities related to the security of the operation of the financial intermediary system, including the following activities**:
   i. for identification, prevention and examination of activities which may have a negative effect on the Company, in particular abuse of the products, services and facilities of the Company, (ii) unlawful or otherwise detrimental (planned) activities, (iii) violation of (legal) requirements;
   ii. for prevention, countering or investigation of planned or committed crimes or detrimental conduct against the financial intermediary system, the Company, the Data Subjects or the employees;
   iii. for the operation of security or alert systems used by the actors of the financial intermediary system; or
   iv. for the performance of legal obligations, especially with respect to obligations related to the prevention of money laundering and terrorism.

When the issue arises as to whether the processing of personal data for the above purposes is lawful, the Data Protection Officer shall be consulted in writing before commencement of the data processing by the unit carrying out the processing. The Data Protection Officer shall respond within three (3) working days.

3.2.1. Processing of sensitive data

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

Sensitive data may only be collected, used or otherwise processed for the purpose or purposes specified herein:

a) **Personal data revealing racial or ethnic origin** – The Company may process CCTV-footage (i) for the identification of Data Subjects, business partners or suppliers; (ii) for security reasons; and/or (iii) for the performance of legal obligations;
b) **Criminal data** – (including data related to unlawful conduct or data retrieved from the criminal records):
    i. for the protection of the Company, the financial intermediary system as well as the employees against crimes committed or suspected to be committed in the future;
    ii. for the protection, safety and integrity of the Company, the financial intermediary system as well as the employees;
    iii. for the performance of legal obligations (including especially obligations related to the prevention of money laundering and terrorism).

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 sensitive data;
b) with respect to sensitive data manifestly made public by the data subject;
c) it is possible or obligatory in accordance with a 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, where it is not possible to obtain the data subject's consent.

If sensitive data are processed pursuant to the consent of the Data Subject, data processing shall be subject to the prior consent of the Data Protection Officer. The consent of the Data Protection Officer shall be obtained before commencement of the data processing by the unit carrying out the processing. The Data Protection Officer shall respond within three (3) working days.

3.3. Data retention period

Personal data are stored at the Company only for the below period:

a) period necessary for achieving the legitimate purpose for which the personal data are processed, or
b) period necessary for compliance with the applicable legal requirements.

The Company may set a period (such as minimum retention period, scheduling of the data storage) during which the processing of personal data in a specified category may be performed.

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

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

The Data Protection Officer shall record deadlines set for the erasure of different data

categories in the records of processing activities in accordance with the relevant instructions of the CEO.

4. Accountability and records of processing activities

In accordance with the accountability principle, the Company shall demonstrate compliance with data protection regulations, in particular by maintaining the records of processing activities under Article 30 of the GDPR. The Company shall maintain the records of processing activities (including its electronic form) in writing. The record 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) Data Subjects, and the categories of personal data concerned;
d) the categories of recipients to whom the personal data have been or will be disclosed, including their geographic location;
e) if personal data are transferred to countries which do not provide an adequate level of protection or if the transfer is based on an adequacy decision, then the appropriate safeguards applicable to the country which does not provide an adequate level or protection or in the case of transfer based on an adequacy decision the destination country or non-compliant country;
f) where possible, the envisaged time limits for erasure of the different categories of data; and
g) where possible, a general description of the technical and organisational security measures.

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

5. Data security

The Company shall ensure 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 security of Personal Data, in particular protection against unauthorized or unlawful processing of data, accidental loss, destruction or damage.

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 this Regulation and protection needs.

Enforcement of Data security rules shall be ensured by the Company via separate regulations, instructions and rules of procedure. In order to enforce the terms of Data security, the company shall provide affected employees with appropriate training.

When defining and applying measures ensuring the security of Data, the Company shall take into account the state of technology. From the different possible data processing

solutions, it shall choose the one which ensures the highest level of protection, unless it would constitute a disproportionate burden.

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

6. Personal data breach

All Employees shall report to the Data Protection Officer (Schedule No. 3 of this Regulation) possibly in writing if they become aware of an incident which may endanger Data Security, a personal data breach or the possibility of its occurrence immediately after having become aware of it.

Third persons may report personal data breaches occurred with respect to the data processed by the Company, and or the data processor acting on behalf of the Company to the following address which is available at the Company's website: infosec@exim.hu.

The Data Protection Officer shall examine the reported personal data breach within 24 (twenty-four) hours in order to determine whether risk exists that the Data Subjects may not enforce their rights. If it is not probable, then he or she shall decide whether the other professional units are to be notified of the report in question. If based on the report it is justified to involve other professional 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 examination it turns out that there is a risk that the data subjects' rights may not be enforced, the Data Protection Officer shall report the personal data breach to the Authority without undue delay after becoming aware of a personal data breach, but no later than within seventy-two (72) hours.

The Data Protection Officer shall include the following in the report submitted to the Authority:

- content of the personal data breach, including the categories of Data Subjects and the categories of data affected by the breach,
- communicate the name and contact details of the data protection officer or other contact person where more information can be obtained;
- describe the likely consequences of the personal data breach;
- describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

The Data Protection Officer shall maintain records on personal data breaches (Annex No. 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 erasure of entries older than 10 years. The records concerning personal data breaches shall contain the following information:

- Categories of data affected by the personal data breach;

- Categories 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;
- Implemented measures;
- Other data.

When the personal data breach is likely to result in a high risk to the enforcement of the basic rights of natural persons (high risk personal data breach), the Company shall communicate the personal data breach to the Data Subject without delay.

The Company shall not inform the Data Subject if:

- the Company has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption; and the Data Protection Officer may request the opinion of the head of the IT with respect to the adequacy of such measures, if necessary
- basic rights of Data Subjects are no longer likely to materialise.

If necessary, the Data Protection Officer shall provide a written statement on this.

- directly informing the Data Subject would involve disproportionate effort, and therefore the Company shall provide a public communication (internet) whereby the Data Subjects are informed on the personal data breach in an adequate manner. The Data Protection Officer shall decide whether this method of information provision may be applied.

7. Processor

The Company may engage a Processor on the basis of a permanent or an ad-hoc assignment. Processors may be engaged on a permanent basis primarily if it 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. If a Processor is engaged, legal regulations concerning data protection and in particular the provisions of the GDPR shall apply. Processors may be engaged exclusively on the basis of a written agreement which shall provide for tasks related to Data Protection and Data Security. The template for the contract to be concluded with the Processor is included in Schedule No. 7 of this Regulation.

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 instructions concerning data processing activities.

If in accordance with the contract concluded with the processor personal data are processed, then the contract may only be concluded if the Data Subject person involved in the processing, including cooperating subcontractors, sub-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 of checking such compliance. This statement shall be made within the data processing agreement included in Schedule No. 7 of this Regulation, and shall be stored together with the contracting or agency agreement (Basic Agreement).

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 engage another Processor only with the approval of the Company.

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

With the conclusion of the contract included in Schedule No. 7, the Company ensures that, during the activities of the Processor, Data Subjects' rights are not violated, and the Processor may only become aware of data if it is absolutely necessary for the performance of its task.

The Company may only engage persons or organisations with data processing who or which provide adequate safeguards for the implementation of technical and organisational measures appropriate for the lawfulness of data processing and the protection of Data Subjects' rights.

In order to demonstrate such safeguards, in accordance with the rules of data protection impact assessment the data processor shall fill in the form included in Schedule No. 8 and submit it to the controller before commencement of 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. In accordance with Article 28 of the GDPR, the contract to be concluded between the Company and the Process under Schedule No. 7 shall include at least the following:

a) Statement of the Processor according to which it has implemented the technical and organisational measures necessary for the protection of the Data Subjects' rights;

b) The processor shall not engage another processor (sub-processor) without prior specific or general written authorisation of the Company.

c) The subject-matter and duration of the processing carried out by the Processor, the nature and purpose of the processing, the type of personal data and categories of Data Subjects;

d) The Processor's consent according to which it processes the personal data only on documented instructions from the Company, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the provider of the outsourced activity is subject;

e) The Processor shall assist the Company to respond requests for exercising the data

subjects' rights;

f) The Processor shall undertake in a separate clause to keep personal data confidential and implement the data security measures required by the GDPR;

g) The commitment of the Processor according to which at the choice of the Company, it deletes or returns all the personal data to the Company after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;

h) The commitment of the Processor according to which it ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

The Processor shall maintain records on its processing activities performed on behalf of the Company under Article 30 of the GDPR, and shall inform the Company immediately in all cases where it has become aware of the violation of rules concerning the processing of personal data.

The Company makes all information available which may be necessary for demonstration of performance of the obligations specified in the GDPR.

The Company shall inform Data Subjects of the Processors before commencement of the processing and/or upon subsequent request of Data Subjects. The Company complies with its information duty by publishing a notice under Article 13 of the GDPR on its website within five (5) working days after signing the contract concluded with the Processor. The publication of the notice shall be initiated by the organisational unit responsible for the conclusion of the contract by contacting the Data Protection Officer, who shall prepare the notice immediately but no later than three (3) working days within the conclusion of the contract and send it to the Marketing and Communications unit which shall ensure its publication of the website. The Data Protection Officer shall record the Processors (name, registered office) in the electronic data protection register maintained by him or her. The Data Protection Officer shall record the Processors in the data protection register maintained by him or her

Within five (5) working days after 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 enforce them.

8. Outsourcing

The Company may outsource any activities related to its financial and auxiliary financial service activities, or such activities as it is ordered 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 are protected at the

person performing the outsourced activity.

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

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

9. Data transfer

If there is no legal provision stipulating otherwise, the Company may comply with requests of third parties outside the Company for data provision only if the Data Subject grants his or her consent in writing. The Data Subject may grant such consent in advance for a specific period, purpose or certain bodies which may submit such a request. The Data Protection Officer shall retain the consent during the period of Processing and for ten (10) years after its termination, and shall ensure disclosure of the Data.

Requests submitted by third persons based on statutory authorisation, which are sent by authorities acting in criminal proceedings (police, court, prosecutor's office), the National Tax and Customs Administration of Hungary, and national security services, shall be complied with regardless of the Data Subject's consent. The head of the organisational unit which performs the request shall immediately inform the CEO and the Data Protection Officer of the request on the next working day after receipt of the request electronically. Data provision may be performed in accordance with the opinion of the Data Protection Officer upon notice of the CEO. The CEO may lodge a complaint which does not have a suspensory effect with the competent minister against the request of the national security services for data provision.

The head of the competent organisational unit shall record data transfers to third parties, and shall send such records to the Data Protection Officer within one (1) working day after the data transfer. The Company's records of processing activities under Article 30 of the GDPR shall contain the data transfers.

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

9.1. Data transfer abroad

For certain data processing activities, the Company may transfer data to third countries outside the European Economic Area or international organisations ('**Data transfer abroad**'). Data transfers abroad shall always be approved by the Data Protection Officer.

Data transfers abroad may only occur if the European Commission ('**Commission**') has stated that the third country ensures an adequate level of protection for the personal data ('**Adequacy Decision**').1

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

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

the processing. Such safeguards may include the following – without the specific authorisation of the competent supervisory authority:

- standard data protection clauses adopted by the Commission, and/or standard data protection clauses adopted by the supervisory authority and approved by the Commission;
- an approved code of conduct together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards Data Subjects' rights;
- an approved certification mechanism together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards Data Subjects' rights.

In the absence of adequate safeguards, the data transfer may occur if any 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 such transfers for the data subject 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-contractual 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 legal 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, where the data subject is physically or legally incapable of giving consent;
- the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.

Where a transfer could not be based on adequacy, adequate safeguards are not available and none of the deviations concerning the special situations may be applicable, a transfer to a third country may take place only if:

- the transfer is not repetitive,
- concerns only a limited number of Data Subjects,
- is necessary for the purposes of compelling legitimate interests pursued by the controller which 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 personal data.

In such cases, the Data Protection Officer shall immediately inform the supervisory authority of the transfer, and in addition to the general information, he or she shall inform

the Data Subject of the transfer and of the compelling legitimate interests pursued.

10. Information provided to the Data Subjects

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

The Company shall provide Data Subjects with information under Articles 13 and 14 of the GDPR on the processing of their personal data in the form of adequate notices. The information addressed to the Data Subject shall be transparent, concise, easily accessible and easy to understand, and clear and plain language shall be used.

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

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

The Company shall inform the Data Subject of the following:

a) primary and secondary purposes for which personal data are processed and the related legitimate interest of the Company, if applicable;
b) name and contact details of the person responsible for data processing at the Company;
c) nature and categories of the processed personal data;
d) categories of the employees of the Company and third persons to whom personal data are transferred (if applicable);
e) how Data Subjects' rights are enforced, including information on the right to lodge a complaint with the Authority;
f) if personal data are transferred to countries which do not provide an adequate level of protection or if the transfer is based on an adequacy decision, the appropriate safeguards, means of obtaining their copies or their availability;
g) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine 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 requirement necessary to enter into a contract, and the possible consequences of failure to provide such data.

10.2. Information to be provided where personal data are not collected from the Data Subject

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

a) Information set forth in Section 11.1;
b) the (publicly available) source of personal data;
c) the following information:
    - when the personal data are recorded in one of the databases of the Company, but no later than within one month after the collection of the personal data; or

- if personal data are communicated to other recipients, no later than at the first time when personal data are communicated to other recipients.

10.3. Exceptions

Provisions of Section 11.2 shall not apply if

a) where the provision of information to the data subject proves to be impossible or would involve a disproportionate effort; or
b) would involve disproportionate costs; or
c) obtaining or disclosure is expressly laid down by law to which the Company is subject and which provides appropriate measures to protect the data subject's legitimate interests.

The applicability of the above shall be decided by the Data Protection Officer in all cases.

11. The Data Subjects' rights and their enforcement

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

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

Rules of procedure related to Data Subjects' rights are included in Section 12.7 of this Regulation.

11.1. Right to access data

Data Subjects shall have the right to obtain from the Company confirmation as to whether their data are processed by or on behalf of the Company, and such confirmation shall contain the following:

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) source of the personal data where personal data are not collected from the Data Subject;
f) if personal data are transferred to countries which 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 confirmation, the Company shall provide the Data Subject with the following information upon his or her request:

a) the existence of the right to request from the Company rectification or erasure of personal data or restriction of processing of personal data concerning the data

subject or to object to such processing;
b) the right to lodge a complaint with the Authority;
c) the possibility of judicial remedy; and
d) if relevant, the existence of the right to receive compensation for violation of the binding corporate rules

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

11.2. Right to rectification

The Data Subject shall be entitled to request rectification of inaccurate data concerning him or her. Taking into account the purposes of the processing, the Data Subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

11.3. Right to erasure

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

a) the personal data are 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 have been unlawfully processed; or
e) the personal data of the Data Subject have to be erased for compliance with a legal obligation.

11.4. Right to restriction of processing

The Data Subject shall be entitled to request restriction of 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 personal data for the legitimate purposes of the processing, but they are required by the Data Subject for the establishment, exercise or defence of legal claims; or
d) the Data Subject successfully objects to processing of his or her personal data pursuant to Section 12.6, pending the verification whether the Company has legitimate grounds.

If the Data Subject wishes to restrict the processing of his or her personal data, it may have an impact on the services provided by the Company.

Where processing has been restricted, such personal data shall, with the exception of storage, only be processed with the Data Subject's consent or for the establishment,

exercise or defence of legal claims or for the protection of the rights of another natural or legal person.

The Company shall inform the Data Subject before the restriction of processing is lifted.

11.5. 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.

11.6. 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 processing of personal data concerning him or her which is based on performance of a task carried out in the public interest or in the exercise of official authority vested in the Company, and for enforcement of the legitimate interest of the Company or 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.

11.7. Provisions related to the exercise of Data Subjects' rights

Written, paper-based requests of the Data Subjects shall be filed in accordance with the effective Document Management Regulation, and after the filing, the organisational unit responsible for the filing shall send the request to the Data Protection Officer immediately, but no later than on the working day following the filing. The Marketing and Communications unit shall transfer requests for the exercise of Data Subjects' rights submitted electronically to info@exim.hu within one (1) working day to the Data Protection Officer.

Before examining obligations concerning the fulfilment of the request, if the request is incomplete, the Data Protection Officer shall request the Data Subject to:

a) definition of the type of personal data to which he or she wishes to have access;
b) definition of the circumstances in which the Company has collected the data;
c) satisfactory demonstration of his or her identity; and
d) in the case of requests for rectification, erasure, restriction or objection, definition of the reasons for which the personal data are inaccurate, incomplete, or not processed in accordance with the relevant legal regulations or this Regulation.

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

a) decision of the Company with respect to the submitted request and measures taken

or planned following the request;
b) whether further information or clarification is necessary for the efficient processing of the request; or
c) extension of the deadline and the latest deadline when the Company shall inform the Data Subject of its decision, which shall not exceed one month of receipt of the request.

The Data Protection Officer shall prepare the draft response, if necessary with the involvement of the Legal Services and the unit performing the data processing. If the Legal Services and the affected unit are involved, they shall have at least three (3) working days.

If the Company does not take action on the request of the data subject, the Company shall inform the data subject without delay and at the latest within one (1) month of receipt of the request of the following:
a) the reasons for not taking action;
b) and of the possibility of lodging a complaint with the Authority; and
c) seeking a judicial remedy.

The Data Protection Officer shall record the requests submitted to the Company electronically in his or her own organisational folder.

If, based on the Data Subject's request, information shall be provided or measure shall be taken, the Data Protection Officer shall immediately notify the affected organisational unit thereof.

The Company shall provide information and measures following the exercise of Data Subjects' rights for free. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, in accordance with the relevant opinion of the Data Protection Officer, the Company may either charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or refuse to provide information or act on the request.

The head of Accounting shall set the amount of reimbursement by taking into account the costs specified in Schedule No. 2 of this Regulation, and the Company shall inform the Data Subject thereof 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 reimbursement to the Company within the deadline indicated on the invoice issued by the Company, by bank remittance to the bank account number indicated on the invoice.

If the request for data entails the reimbursement of costs, the Data Protection Officer shall request information on the amount of costs electronically from the Accounting within three (3) working days. The Accounting shall inform the Data Protection Officer of the costs of data provision within one (1) working day, and the Data Protection Officer shall send the prior information concerning the amount of 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. The Company shall reimburse costs already paid if the Company has processed

the personal data unlawfully or if the request for information has led to rectification.

In all cases, the CEO shall decide on the provision of information, taking or refusal of measures, in accordance with the opinion of the Data Protection Officer and the head of the Legal Services.

11.8. Judicial remedy

If the Company does not handle the Data Subject's request for exercise of his or her rights related to the processing of personal data, or fails to provide a response on the procedural acts related to the request or their results within three (3) 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 set forth in the GDPR, the Data Subject may seek judicial remedy before the courts of the Member State where the data subject has his or her habitual residence.

11.9. Compensation, indemnification

The Data Subject and any other person who has suffered material and non-material damage due to the violation of the data protection and data security provisions of this Regulation or the GDPR, may claim compensation and indemnification from the Company, and/or the Processor carrying out data processing activities on a contractual basis on behalf of the Company.

The Company shall be liable towards the Data Subject for damage caused by the Processor engaged by the Company, and the Company shall pay the compensation to which the Data Subject is entitled in the case of an infringement of personality rights committed by the Processor.

In the cases indicated in Article 82 of the GDPR, the Company may be exempted from the obligation to pay compensation and indemnification.

12. Disclosure of Personal Data

The disclosure of Personal Data processed by the organisational units is prohibited, unless authorised by the Data Subject, and/or stipulated by law. Aggregated statistical data which are partly based on the personal data of the Company's Employees, Suppliers, Sponsored Parties and/or Clients may be disclosed, provided that the Data Subject cannot be recognised from such data. Before disclosure of Personal Data, the Employee of the Company shall ensure that the Data Subject cannot be identified based on the disclosed Personal Data. In case of doubt, the Data Protection Officer shall be consulted in writing.

13. Performance of interest assessment tests

Personal data may be processed if the Data Subject's consent cannot be obtained or involves excessive cots, 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 'overrule' 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 based

on the comparison of such rights. The interest assessment test shall be carried out by the Data Protection Officer based on consultation with the organisational unit 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.

14. Disclosure of and access to data of public interest and data accessible on the grounds of public interest

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

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

15. Closing provisions

Upon entry into force of this Regulation, the CEO Directive no. 5/2018 on the Data Protection and Data Security Regulation of the Company is repealed.

Person responsible for reviewing the regulation: Data Protection Officer.

The Data Protection Officer shall review this Regulation 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, 12.06.2018