INTERNAL RULES ON COLLECTION, PROCESSING, ARCHIVING, STORAGE, DESTRUCTION AND PROTECTION OF PERSONAL DATA IN THE REGISTER OF COUNTERPARTIES AND PROCEDURE FOR THE EXERCISE OF THE RIGHTS OF DATA

SUBJECTS SECTION I

GENERAL PROVISIONS

Subject matter

Article 1.

/1/ These Rules (hereinafter referred to as Rules/the Rules) are issued by TGSOFT Ltd as a personal data controller (hereinafter also referred to as Controller).

/2/ The Rules shall determine the procedure for collection, processing, storage, archiving, destruction and protection of personal data by the Controller in connection with the conclusion, modification, performance, termination/rescission of commercial /civil/ contracts between TGSOFT Ltd and third parties, as well as in connection with any other annex, additional agreement and/or protocol establishing legal relationships with a third party, except in in the case of employment and/or civil contracts with natural persons.

/3/ The rules shall regulate the rights, obligations and responsibility in the event of nonfulfillment of the obligations by:

1. data subjects – natural persons who are party to a specific commercial contract concluded with the Controller; natural persons who represent or are employees of a counterparty of the Controller; natural persons whose personal data the Controller collects, processes, stores and destroys by virtue of their explicit consent given for and upon the exercise of its lawful activity and in protection of its legitimate interest relating to selection or other inquiry with a view to future, potential establishment of an employment or other legal relationship; natural persons whose personal data the Controller collects, processes, stores and destroys by virtue of a contract and/or another form assigning to it an activity of selection and/or other inquiry with a view to future, potential establishment of an employment relationship between the counterparty and the respective natural persons;

2. data processors – the employees who, in the performance of their function or by order of the Controller, collect, process, store, archive or destroy personal data /data processors/;

3. data users – natural persons, legal persons and/or bodies performing public functions who/which, by virtue of a law or the internal rules of the Controller, have access to the personal data /data users/.

Article 2.

/1/ The rules shall regulate:

1. The procedure for keeping, maintaining and protecting personal data in the Register of Counterparties.

2. The procedure and rules for collecting, processing, storing, archiving, destroying the personal data by TGSOFT Ltd as a controller and/or processor.

3. The rights and obligations of the data processors and users, their responsibility in the event of non-fulfillment of these obligations in the Register of Counterparties.

4. The procedure and rules for the implementation of the rights of information of the data subjects whose personal data are collected, processed, stored, archived, destroyed in the Register of Counterparties.

5. The procedure and rules for the implementation of the right of access of data subjects, public authorities and third parties to the personal data that are collected, processed and stored in the Register of Counterparties.

6. The procedure and rules for the implementation of the right of data subjects to rectification and supplementing of inaccurate and/or incomplete personal data that are processed, stored, archived, destroyed in the Register of Counterparties.

7. The procedure and rules for the implementation of the right of data subjects to erasure of the personal data (the right to be forgotten) that are processed, stored, archived, destroyed in the Register of Counterparties.

8. The procedure and rules for the implementation of the right of data subjects to object processing of the personal data that are processed, stored, archived, destroyed in the Register of Counterparties, including the objection that personal data should not be subject to an automated decision which includes profiling.

9. The procedure and rules for the implementation of the right of data subjects to notification in case of breach of the security of the personal data that are processed, stored, archived, destroyed in the Register of Counterparties.

10. The procedure and rules for the implementation of the relationships of TGSOFT Ltd , as a controller, with the Commission for Personal Data Protection.

Purpose of the Rules

Article 3.

/1/ The purpose of the Rules is to create a legal form and organization, which shall ensure and guarantee the collection, processing, storage, archiving and destruction of personal data in full compliance with the requirements of Regulation 2016/679, the Personal Data Protection Act, the regulations on their implementation and the instructions of the Commission for Personal Data Protection.

/2/ The purpose of the Rules is to create a legal form and organization in the process of collecting, processing, storing, archiving and destroying the personal data that will fully guarantee their protection and security within the meaning of Regulation 2016/679, the Personal Data Protection Act, the regulations on their implementation and the instructions of the Commission for Personal Data Protection.

/3/ The purpose of the Rules is to create a procedure and organization for the exercise of the right to information, access, rectification and supplementing, erasure, objection and notification in the event of a security breach, which will ensure and guarantee to the data subjects their lawful and effective implementation. Compliance of the Rules with Regulation 2016/679, the Personal Data Protection Act and other regulatory acts

Article 4.

/1/ The Rules are issued by TGSOFT Ltd pursuant to Regulation 2016/679, the Personal Data Protection Act /PDPA/, in conjunction with Article 4 of Ordinance No. 1 of 30 January 2013 on the minimum level of technical and organizational measures and the permissible type of personal data protection, issued by the Chairman of the Commission for Personal Data Protection and in fulfillment of his duties as a data controller.

/2/ Upon amendment to the provisions of the regulatory acts mentioned in the previous paragraph or other regulatory acts specified in these Rules, the Controller must, within 10 working days after their promulgation, make the necessary changes to the latter.

/3/ In the event that the Controller does not make the necessary changes to the Rules and does not bring their content into line with the amendments to the PDPA and/or other regulatory acts, the data processors, data subjects, as well as all other persons who are their addressees shall be entitled to refuse to fulfill the obligations arising from the relevant texts that do not comply with the regulatory framework.

SECTION II APPLICATION OF THE INTERNAL RULES

Effect of the Rules over time

Article 5. The Rules shall enter into force on the date of their approval.

Effect of the Rules on persons

Article 6.

/1/ The Rules shall apply to:

1. The Controller, the data processors, the users, the persons to whom the Controller provides access, as well as to all third parties who, by virtue of a law, are entitled to access to another person's data that are collected, processed, stored, archived and destroyed in the Register of Counterparties.

2. all natural persons who are representatives or a party to an existing commercial /civil/ contract concluded with the Controller; natural persons who are employees of a current counterparty of the Controller, whose personal data are already collected, processed, stored, archived and destroyed or are to be collected, processed, stored, archived and destroyed in the Register of Counterparties,

3. all natural persons who are a party to a specific terminated/rescinded/performed commercial /civil/ contract concluded with the Controller or natural persons who are employees of a former counterparty of the Controller, whose personal data are collected, processed, stored, archived in the Register of Counterparties and not have been destroyed and/or transmitted to other state authorities, including the relevant state archives for storage /if they are subject to it/.

4. all natural persons whose personal data the Controller collects, processes, stores and destroys by virtue of their express consent given for and in the exercise of its lawful activity and in protection of its legitimate interest relating to the selection or other inquiry with a view to future, potential establishment of an employment or other legal relationship;

5. all natural persons whose personal data the Controller collects, processes, stores and destroys by virtue of a contract and/or other form assigning to it an activity of selection and/or other inquiry with a view to future, potential establishment of an employment relationship between a counterparty of the Controller and the respective natural persons.

6. All subjects that are not explicitly mentioned in the previous paragraphs for whom the Rules give rise to obligations, rights or responsibilities.

/2/ The Rules shall enter into force and give rise to rights, obligations and responsibilities from the date of the persons' acquaintance with their content.

/3/ The Controller shall bring the Rules to the knowledge of the abovementioned persons within 10 working days from their adoption.

SECTION III TYPES OF PERSONAL DATA THAT ARE COLLECTED, PROCESSED, STORED, ARCHIVED AND DESTROYED IN THE REGISTER OF COUNTERPARTIES

Personal data on physical identity

Article 7.

/1/ The Controller shall collect, process, store, archive and destroy personal data on the physical identity of the subjects as follows: full names, personal identification number, number of identity card or other identity document, date and place of issue, up-to-date permanent address, current address, telephone number, name and position of a contact person.

/2/ The personal data are necessary for the lawful implementation of the rights and obligations of the Controller and its counterparties, including for conclusion, modification, performance, termination/rescission of commercial contracts between TGSOFT Ltd and its counterparties, as well as any other contract establishing relationships with a third party /except in the cases of an employment and/or civil contract with a natural person/; for contacting the representatives of the respective counterparty regarding the performance, termination/rescission of the relevant legal relationship; for implementation of its lawful activity and in protection of its legitimate interest relating to selection or other inquiry with a view to future, potential establishment of an employment or other legal relationship; for implementation of the activities for selection and/or other inquiry assigned with the commercial contract with a view to future, potential establishment of an employment relationship between the counterparty of the Controller and the respective natural persons, etc.

/3/ The personal data shall be provided on the basis of the fulfillment of obligations that are assigned in the respective commercial contract concluded with the counterparty under the Commercial Act (CA), the Obligations and Contracts Act (OCA), the Health and Safety at Work Act (HSWA), the Accountancy Act (AA), the Value Added Tax Act (VAT Act), the Corporate Income Tax Act (CITA), and the regulations on their implementation. Personal data on representative functions, professional activity and bank accounts

Article 8.

/1/ The Controller shall collect, process and store personal data on representative functions, professional activity such as: exercised representative functions, occupied positions, performed functions, completed projects, type, content and status of the projects /national, international/, bank account numbers, correspondence addresses for the implementation of the activities assigned with a commercial contract; professional qualification, professional experience and other personal data for the purposes of its lawful activity and in protection of its legitimate interest relating to selection or other inquiry with a view to future, potential establishment of an employment or other legal relationship for which the subjects have given it their explicit consent; professional qualification, professional experience and other personal data for the purposes of selection and/or other inquiry with a view to future, potential establishment of an employment relationship between the counterparty of the Controller and the respective natural persons are designated/agreed between the Controller and the counterparty, etc.

/2/ The personal data are necessary for the lawful implementation of the rights and obligations of the Controller and its counterparties in the respective legal relationship, including for conclusion, modification, performance, termination/rescission of commercial contracts between TGSOFT Ltd .

and third parties, as well as any other contract establishing legal relationships with a third party /except in the cases of an employment and/or civil contract with a natural person/; contacting the representatives of the respective counterparty in connection with the performance, termination/rescission of the relevant legal relationship; for the purposes of his lawful activity and in protection of its legitimate interest relating to selection or other inquiry with a view to the future, potential establishment of an employment or other legal relationship for which the subjects have given it their explicit consent; for carrying out the selection and/or other inquiry with a view to the future, potential establishment of an employment relationship between the counterparty of the Controller and the respective natural persons in the execution of a contract between the Controller and the counterparty, etc.

/3/ The personal data are provided on the basis of fulfillment of normative obligations, set out in the respective contract concluded with the third party, the Commercial Act (CA), the Obligations and Contracts Act (OCA), the Health and Safety at Work Act (HSWA), the Accountancy Act (AA), the Value Added Tax Act (VAT Act), the Corporate Income Tax Act (CITA), and the regulations on their implementation.

SECTION IV DOCUMENTS COLLECTED, PROCESSED AND STORED IN THE REGISTER OF COUNTERPARTIES

Purpose of the documents

Article 9.

/1/ All the personal data which are necessary for the Controller for the lawful conclusion, modification, performance, termination/rescission of commercial /civil/ contracts between TGSOFT Ltd and third parties, as well as any other contract establishing legal relationships with a third party /except in the cases of an employment and/or civil contract with a natural person/ shall be collected, processed, stored, archived and destroyed in the Register of Counterparties.

/2/ The personal data which the Controller must obtain in the fulfillment of its obligations under the the Commercial Act (CA), the Obligations and Contracts Act (OCA), the Health and Safety at Work Act (HSWA), the Accountancy Act (AA), the Value Added Tax Act (VAT Act), the Corporate Income Tax Act (CITA), and the regulations on their implementation, etc. shall be collected, processed, stored, archived and destroyed in the Register of Counterparties.

/3/ The personal data which are specified/agreed in the contract between the Controller and the counterparty and are necessary for carrying out the selection and/or other inquiry with a view to future, potential establishment of an employment relationship between the counterparty of the Controller and the respective natural persons shall be collected, processed, stored, archived and destroyed in the Register of Counterparties.

/4/ The personal data for which the subjects have given the Controller their explicit consent for the purposes of its lawful activity and in protection of its legitimate interest relating to selection or other

inquiry with a view to future, potential establishment of an employment or other relationship shall be collected, processed, stored, archived and destroyed in the Register of Counterparties.

/5/ The personal data which the Controller, by virtue of its internal acts, rules, statutes and at its discretion, receives in order to protect effectively its interests relating to the conclusion, modification, performance, termination/ rescission of commercial /civil/ contracts between TGSOFT Ltd and third parties, as well as any other contract establishing relationships with a third party /other than the cases of an employment and/or civil contract with a natural person/ shall be collected, processed, stored, archived and destroyed in the Register of Counterparties.

/6/ The types of documents which, by virtue of a law, regulation or an act of the Controller, are necessary to enable the lawful implementation of the subjective rights and obligations of employees and contractors shall be collected, processed, stored, archived and destroyed in the Register of Counterparties.

Main types of documents

Article 10.

/1/ TGSOFT Ltd , as a controller within the meaning of Article 3 (1) of the PDPA, shall be entitled to request, collect, process and store the following documents: 1. Identity documents for the identification of the respective counterparty, where it is required by law. 2. Certificate of good standing or excerpts from the relevant registers (for example, Commercial Register and Register of Non-Profit Legal Entities). 3. Bank account certificate; invoices relating to price payment; statements required by law. 4. Documents for which the subjects have given their explicit consent. 5. Documents which are specified/agreed in the contract between the Controller and the counterparty and are necessary for the selection and/or other inquiry with a view to future, potential establishment of an employment relationship between the counterparty of the Controller and the respective natural persons.

/2/ In case of failure to provide the originals of the documents, copies thereof that duly guarantee the conformity to the original content may also be processed with the consent of the controller.

/3/ If it is necessary the relevant supporting documents to be kept by the controller, originals or copies thereof may be provided.

/4/ The listing of the required documents is not exhaustive and the data controller may request other documents in connection with the data that are subject to processing. SECTION V PERSONS RELATED TO THE REGISTER OF COUNTERPARTIES Processors of personal data in the Register of Counterparties Article 11. A data processor for the purposes of these Rules shall be the natural or legal person who/which, by office, order or contract, updates, records, modifies, organizes, copies, completes, stores, maintains, uses personal data, makes inquiries, obtains information from personal data in connection with the processing of the documentation of the controller, stores, archives, deletes, destroys and otherwise treats the personal data in the Register of Counterparties.

Article 12.

/1/ Data processors of the Register of Counterparties shall be the employees holding the position: assistant junior specialist of human resources, junior specialist of human resources, specialist of human resources, team leader.

/2/ The rights and obligations of the processors of personal data in the Register of Counterparties shall be regulated in these rules, in the job descriptions, in the statements that they have signed (Appendix No. 1), in the orders of the controller and other procedures of TGSOFT Ltd .

Obligations of the data processor

Article 13. The data processor shall have the following obligations:

1. to collect, process, store, archive and destroy the personal data in the Register of Counterparties, subject to the requirements of Regulation 2016/679, the PDPA, these Rules, the statements signed and the orders of the Controller.

2. to collect only the personal data determined by type and content, as well as to process, store, archive and destroy them for the purposes and in the manner determined by the Controller.

3. to collect, process, store, archive and destroy the personal data in the Register of Counterparties in such a manner as to prevent their disclosing, submitting or making known to third parties who are not entitled to it.

4. to collect, process, store, archive and destroy the personal data in the Register of Counterparties in a manner that guarantees their security and protection.

5. to interact with the other processors in the collection, processing, storage, archiving and destruction of the personal data in a manner that guarantees the application of the PDPA and these Rules.

6. to inform in the manner described in these Rules any natural person whose personal data are collected in the Register of Counterparties.

7. to ensure that the natural persons complete the written documents that are required upon informing, to collect and store the written documents completed by them.

8. to implement the right of access of any natural person to his or her personal data in the Register of Counterparties in the manner described in these Rules.

9. to implement the right of rectification, of erasure /right to be forgotten/, objection of any natural person regarding the collected, processed, stored, archived personal data in the Register of Counterparties in the manner described in these Rules.

10. to keep and complete the Register for the exercise of the rights of data subjects in the manner described in these Rules.

11. to file duly in the Register for the exercise of the rights of data subjects any submitted application for the exercise of the relevant right, to examine it and check its lawfulness within the stipulated time limit, to draw up a refusal, a reply, a certificate for the provision of the requested information, to serve on the person the requested and/or provided information.

12. to inform the data protection officer of any breach of these Rules, of any risk or danger to the security and confidentiality of the personal data that become known or available to it.

Obligation to keep secret the available personal data

Article 14.

/1/ All personal data from the Register of Counterparties, which become available to the data processors during or in connection with the performance of their duties, shall be confidential information of the highest sensitivity for the employer as a data controller.

/2/ The personal data from the Register of Counterparties may not be disclosed in any form and to anyone, may not be shared, discussed, commented on, used, interpreted during and after the termination of the activities for their collection, processing, storage, archiving and destruction.

/3/ The data processors shall be responsible to the controller and the respective natural person for any material and/or non-material damage caused as a result of improper actions or inactions related to a breach of the rules on protection and confidentiality, where the damage is a direct and immediate consequence of the actions/inactions of the data processor, user, or data protection officer.

/4/ Disciplinary responsibility may also be imposed on data processors, if they are subject to such responsibility, including disciplinary dismissal.

/5/ As a controller, TGSOFT Ltd shall ensure the protection of the personal data in the area by means of controlling access to the building and the work premises with individual cards for each employee/contractor, a key and special access mode for outside visitors.

Obligation to treat personal data lawfully and correctly

Article 15.

/1/ The data processors, users and data protection officers must treat the personal data from the Register of Counterparties only within the statutory purposes and the purposes determined by the controller, while preserving their authenticity, completeness and accuracy.

/2/ The personal data from the Register of Counterparties shall not be altered, supplemented, deleted at the discretion of the data processors, users and data protection officers without an explicit decision of the controller, a change in the current legislation or in these Rules.

/3/ The processors, users and data protection officers shall be responsible to the Controller or the respective natural person for any material and/or non-material damage caused as a result of

improper actions or inactions related to the change, supplementing, deletion of personal data, where the damage is the direct and immediate consequence of the actions/inactions of the processor, user or data protection officer.

SECTION VII INFORMING THE SUBJECTS WHOSE PERSONAL DATA ARE COLLECTED IN THE REGISTER OF COUNTERPARTIES

Content of the obligation to inform

Article 16. The Controller must inform each natural person before collecting his or her personal data about the following circumstances:

1. The data that he or she has provided are personal data within the meaning of the PDPA and as such they are subject to special protection arrangements.

2. Pursuant to Regulation 2016/679 and the PDPA, any person has a right of access to the documents that contain his or her personal data, subject also to these Rules.

3. Pursuant to Regulation 2016/679 and the PDPA, any person has a right to rectification of the collected personal data when they are incorrect, incomplete, inaccurate.

4. Pursuant to Regulation 2016/679 and the PDPA, any person has a right of erasure (right to be forgotten), right to object to the processing of personal data, right to object to the disclosure or use of his or her personal data for direct marketing purposes, right to be notified prior to the first disclosure of his or her personal data for direct marketing purposes.

5. Pursuant to Regulation 2016/679 and the PDPA, any person has a right to be informed in the event of a breach of the security of his or her personal data and of his or her right to file a complaint with the Commission for Personal Data Protection.

6. The Controller undertakes to collect, process, store, archive, destroy, use and grant access to his or her personal data for the sole purpose of the implementation of the rights and obligations under the employment /civil/ legal relationship.

7. The Controller undertakes to collect, process, store, archive, destroy, use and grant access to his or her personal data, guaranteeing that they are kept secret from other employees or third parties and ensuring their security and protection.

8. The Controller undertakes not to disclose the personal data to third parties, except with the written consent of the person or in cases specified in a statutory act.

Persons who fulfill the obligation to inform

Article 17. The obligation to inform shall be fulfilled by the following positions: assistant junior specialist of human resources, junior specialist of human resources, specialist of human resources, team leader.

Fulfillment of the obligation to inform upon collection of personal data

Article 18.

/1/ The Controller must inform about the circumstances referred to in Article 20 any person whose personal data are collected in connection with the establishment of a future commercial or civil legal relationship /other than an employment or civil legal relationship with a natural person/, as well as any person whose personal data are collected in connection with the selection or other form of inquiry in the performance of a contract.

/2/ When sending a request for the submission of a tender/contract offer, the text which constitutes Appendix No. 2 to these Rules shall be written at the end of each contract.

/3/ The obligation to inform shall be fulfilled by the following positions: assistant junior specialist of human resources, junior specialist of human resources, specialist of human resources, team leader.

/4/ The manager of TGSOFT Ltd shall exercise incidental and ongoing control over the manner in which the obligation to inform is fulfilled, in compliance with the manner set out in the Rules.

SECTION VIII COLLECTION OF PERSONAL DATA

Initial collection of personal data

Article 19.

/1/ The personal data in the Register of Counterparties shall be collected before the relevant legal relationship is established and/or modified.

/2/ The personal data shall be collected in writing – on paper and/or on a technical medium.

/3/ Only the types of personal data and only the types of written documents that are determined by the Controller shall be collected.

/4/ Provided that a data subject submits personal data or a written document containing personal data which the Controller does not request or prohibit to be collected, the document shall be returned immediately to the subject or, if it is impossible to be returned, shall be immediately destroyed.

/5/ Personal data shall be collected from the following positions: assistant junior specialist of human resources, junior specialist of human resources, specialist of human resources, team leader, subject also to the obligations set out in these Rules.

/6/ Other employees or third parties, outside those mentioned in the previous paragraph, shall not be entitled to collect the personal data from the Register of Counterparties.

/7/ By way of exception, the Controller may, by written order, assign to other employees the collection of personal data. The order shall specify: the persons/positions to whom/which the collection of personal data from the Register of Counterparties is assigned; the period of assignment

and the collection procedure. In this case, the authority assigning the collection of personal data must declare them confidential information and prohibit their disclosure in any form and to anyone, ensuring also that a confidentiality and non-disclosure statement is signed, and acquaintance with these Rules.

/8/ The processors shall not be entitled to collect personal data and written documents containing personal data in the presence of persons who are not processors of the respective personal data or are not users with access to the respective personal data.

Procedure for the initial collection of personal data

Article 20.

/1/ The documents containing personal data shall be collected in one copy and shall be distributed as follows: 1. the original documents shall be returned to the holder: identity documents, bank account certificate, certificates of good standing. 2. documents that remain: contracts, agreements, annexes, offers, notarial acts, invoices, tenders, proposals, statements, extracts from the relevant registers (for example, Commercial Register and Register of Non-Profit Legal Entities), documents on briefings and the like. 3. the documents that are collected for the implementation of selection and/or other form of inquiry in the performance of the lawful activity and in protection of the Controller's legitimate interest, for which the subjects have given their explicit consent. 4. the documents that are collected for the implementation of the selection and/or other form of inquiry in the performance of the contract between the Controller and the counterparty shall be submitted to the counterparty in accordance with the agreed/determined procedure.

/2/ The paper documents remaining with the controller shall be collected and filed in: 1. the dossier kept in connection with the respective legal relationship for which the data are required. 2. the dossiers relating to invoices issued and amounts received.

/3/ The personal data collected from an identity document, bank account certificates, representative functions, positions held shall be entered in: a/ draft documents in an electronic form on the information server; b/ The access to the information server shall be encrypted. Each employee shall connect to the IT systems of TGSOFT Ltd with an individual user name and password, but he or she will also have a personal certificate of access.

/4/ Personal data on a technical media shall be stored in files/directories on the information server, which shall be accessed only by the data processors.

Subsequent collection of personal data

Article 21.

/1/ The Controller shall be entitled at any time to collect personal data that are new and different in kind and content, when they are necessary for the implementation of the rights and obligations of

the counterparties in the respective legal relationships /other than employment or civil ones with natural persons/ or for the implementation of its legal rights and obligations.

/2/ The subsequent collection of personal data shall be subject to full compliance with the requirements of these Rules.

/3/ The subsequent collection of personal data shall be carried out by the data processors referred to in Article 16.

/4/ Other employees or persons, except those that are explicitly stated in the previous paragraph, shall not be entitled to collect personal data.

/5/ The processors shall not be entitled to collect personal data and written documents containing personal data in the presence of persons who are not processors of the respective personal data or are not users with access to the respective personal data.

/6/ The subsequent collection of personal data shall be done in writing (on paper and/or on a technical medium) in the manner described in these Rules.

SECTION IX PROCESSING OF PERSONAL DATA

Processing of personal data

Article 22.

/1/ Processing of personal data in the Register of Counterparties is any use, recording, copying, reproduction on another medium/media, use related to the processing of other types of personal data, updating, maintenance, retaining in the memory, storage, etc. of collected personal data for the purpose of implementing the rights and obligations of the counterparties in commercial or civil legal relationships /other than employment or civil ones with natural persons/ or for the implementation of the legal rights and obligations of the controller.

/2/ Within the meaning of these Rules, processing is ongoing and incidental.

Ongoing processing of personal data

Article 23.

/1/ Ongoing processing of personal data is any processing, irrespective of the frequency /daily, weekly, monthly, every three months, etc./, which is necessary for the implementation of constantly arising rights and obligations of third parties - counterparties in commercial or civil legal relationships /other than employment or civil ones with natural persons/ or of the Controller.

/2/ The ongoing processing of personal data shall be carried out by the data processors referred to in Article 16 of these Rules.

/3/ By way of exception, the Controller may, by written order, assign to other employees to process personal data. The order shall specify: the positions to which the processing of personal data from

the Register of Counterparties is assigned; the assigned period of processing and the processing procedure. In this case, the persons assigning the processing of personal data shall declare them confidential information and shall prohibit their disclosure in any form and to anyone, ensuring also that a confidentiality and non-disclosure statement is signed, and acquaintance with these Rules.

/4/ Employees or other persons outside the designated data processors shall be prohibited from processing the personal data in the Register of Counterparties.

/5/ The data processors must process personal data in person and must personally use and treat the written documents, files, electronic media, which contain the personal data.

/6/ The processors may not transmit, provide, display or make available the content of a written document, file and electronic medium, which contain personal data of persons who are not designated as processors of the respective personal data or are not users with access to the respective personal data.

/7/ The processors are required, after the processing of the documents, folders and other written materials containing personal data, to put them in the designated places or return them in the relevant dossiers.

/8/ The processors are required, after the processing on a technical medium, to close the files or electronic media containing personal data and/or to shut down their computer.

/9/ The processors may not process written documents containing personal data in the presence of persons who are not processors of the respective personal data or are not users with access to the respective personal data.

/10/ After the end of the working time, the processors may not leave any documents, folders, materials, accessible switched on computers, which contain personal data, in their workplaces and in the work premises.

/11/ The processors may not take any type of written documents, folders or materials, computers containing personal data outside of the area of TGSOFT Ltd , except upon notice /permission/ of the controller.

Incidental processing of personal data

Article 24.

/1/ Incidental processing of personal data is any one-time processing that is necessary for the implementation of incidentally arising rights and obligations of employees, contractors and/or of the controller.

/2/ The Controller shall, by written order, specify: the legal grounds on which the incidental processing is assigned and the types of personal data that are subject to such processing; the positions to which incidental processing is assigned; the period of incidental processing; the

position/person providing them with the processed data; special rules for handling personal data; declaring processed personal data as confidential information and prohibiting their disclosure in any form and to anyone.

/3/ The processors may not transmit, provide, display or make available a written document containing personal data, or the content of information made known to them about personal data of persons other than those specified in the order of the controller.

/4/. The processors must, after processing the documents, folders and other materials containing personal data, place them in the respective dossiers.

/5/ The processors may not process written documents containing personal data in the presence of persons who are not processors of the respective personal data or are not users with access to the respective personal data.

/6/ The processors may not leave documents and materials containing personal data in their workplaces and in the work premises after the end of the working time.

/7/ The processors may not carry any type of documents or materials containing personal data outside of the area of the enterprise, except upon notice /permission/ of the Controller.

SECTION X STORAGE OF PERSONAL DATA

Storage of personal data on paper

Article 25.

/1/ Documents on paper containing personal data from the Register of Counterparties shall be stored in the dossier which is kept in connection with the relevant commercial or civil legal relationship in TGSOFT Ltd .

/2/ The dossiers referred to in paragraph 1 shall be stored in special/filing cabinets in the premises, which are the workplace or archive of the data processors.

/3/ The special/filing cabinet shall be locked with a key which shall be stored in a place known only to the data processors who handle the documents from the respective cabinet.

/4/ The data processors who are designated to use the keys may not submit them to other persons, except after an explicit order and/or with the knowledge of the controller.

/5/ The data processors who are designated to use the keys may not leave them unattended in their workplaces, in the work premises, on the doors of the special/filing cabinet.

/6/ The data processors who are designated to use the keys must store the keys in the designated place at the end of the working time.

/7/ The data processors who use the keys may not take them outside of the area of TGSOFT Ltd , except upon notice /permission/ of the controller.

Storage of personal data on a technical medium

Article 26.

/1/ The documents on a technical medium shall be stored on a hard disk and/or a server.

/2/ Only data processors shall have access to personal data files and it shall be protected with a password.

/3/ The access password shall be individual and available only to the personal data processors. The password shall be changed by a controller every 3 months.

/4/ The data processors may not submit their password to other persons, including other data processors, except after an explicit order and/or with the knowledge of the controller.

/5/ The data processors may not make their password available to third parties.

/6/ The software programs which are used in the processing of personal data shall be adapted to the requirements of the PDPA and these Rules. The software program shall contain an antivirus program.

Article 27.

/1/ Each processor shall use an own computer located in a lockable room.

/2/ Only data processors can access the room by means of: A service access card and an own key.

/3/ The designated data processors may not submit their service card or room key to other persons, except after an explicit order and/or with the knowledge of the controller.

/4/ The designated data processors may not leave their service card or room key unattended in their workplaces, in the work premises, or on the doors of the work premises.

SECTION XI ARCHIVING AND DESTRUCTION

Article 28.

/1/ Within the statutory time limit or within the time limit for which the persons have given their explicit consent, the dossiers with all documents containing personal data shall be archived by the data processors.

Article 29.

/1/ The archiving of personal data on a technical medium shall be done on a server and the information shall be encrypted.

Article 30.

/1/ Collected personal data that are not stored and archived shall be destroyed in a way that ensures that they will not be reproduced and/or preserved, and that the data subjects will not be identified.

/2/ Each month, the data processors shall determine the types of personal data and their media that are subject to destruction.

/3/ The data processors shall personally destroy the written documents containing the personal data by means of shredding.

/4/ The data processors shall personally erase the files containing personal data.

/5/ By way of exception, by written order, the controller shall assign to other employees the destruction of the designated personal data. The order shall specify: the positions to which the destruction of the personal data of the Register of Counterparties is assigned; the period of assignment and the destruction procedure. In this case, the persons assigning the destruction of personal data must declare them confidential information and prohibit their disclosure in any form and to anyone, ensuring also that a confidentiality and non-disclosure statement is signed, and acquaintance with these Rules.

/6/ It is prohibited to designate employees or persons other than those designated as data processors for destruction and to destroy the personal data in the Register of Counterparties.

SECTION XII ACCESS TO ANOTHER PERSON'S DATA

Access by state and public authorities

Article 31.

/1/ Access to the personal data in the Register of Counterparties shall be granted to all state or public authorities, which by virtue of a special statutory act are entitled to such access, including, but not limited to: the Commission for Personal Data Protection, the investigation authorities, the prosecutor's office, the court, the State Agency for National Security, the National Revenue Agency, the General Labour Inspectorate Executive Agency, their employees, the Ministry of Interior, etc.

/2/ The Controller must grant the access to the personal data in the Register of Counterparties requested by the state authorities within the scope of their competences without any written or oral permission from their holder.

/3/ Access shall be granted by the respective data processor or officer responsible for the protection of the personal data in the Register of Counterparties.

/4/ Access shall be granted to personal data and the documents containing them as specified by the authority.

/5/ In cases where expert examinations are assigned in proceedings conducted by or against the controller, access for the respective expert/experts shall be allowed only on presentation of an explicit document issued by the authority wherein the respective proceedings are pending, indicating the type and the tasks of the assigned expert examination or the type and nature of the personal

data and the type and nature of the documents containing them and after signing a confidentiality statement by the expert (Appendix No. 3).

/6/ Access shall be granted after notification to the controller, who will assess the lawfulness of the requested access in view of the availability of the relevant personal data.

/7/ The officials shall be provided with the document personally and in such a way as to guarantee the protection of the personal data in them.

/8/ The right of access of officials from a state or public authority shall be exercised in the presence of the following positions: assistant junior specialist of human resources, junior specialist of human resources, specialist of human resources, team leader, who shall not interfere with the activities of the competent authorities, but shall perform the controller's duties related to the preservation and protection of provided personal data within the meaning of the Personal Data Protection Act.

SECTION XII RIGHT OF ACCESS, RECTIFICATION, OBJECTION, ERASURE OF PERSONAL DATA

Right of access to own personal data

Article 32.

/1/ Any person whose personal data are available in the Register of Counterparties shall have the right of access, rectification, objection and erasure.

/2/ Access to their personal data, rectification of the collected and stored personal data, objection to the collection of personal data and erasure of the collected and stored personal data shall have: the natural persons-counterparties; the natural persons-legal representatives of counterparties; the natural persons-attorneys of counterparties, employees of counterparties; the natural persons who have given their explicit consent to participate in the selection or other form of inquiry in the framework of the implemented legal activity and legitimate interest of TGSOFT Ltd ; the natural persons who have participated in the selection and/or other form of inquiry in the performance of a contract between the Controller and its counterparty.

Article 33.

/1/ A person who requests access or rectification, objects or requests erasure should state it personally.

/2/ The person shall complete an application for access, rectification, objection or erasure in a standard form approved by the controller /Appendix No. 4/.

/3/ The application shall be in writing and shall have the following content: 1. Name, address and other data required for the controller to identify him or her. Information about the current address /which is also the correspondence address/, telephone, fax, etc. 2. Indication of the right which he or she wishes to exercise and a description of the information which he or she wishes to obtain, to be

rectified, to which he or she objects or wishes to be erased. 3. Signature, date of submission of the application.

/4/ Granting of access, rectification, objection and erasure without a duly completed application are prohibited.

Article 34. If the person requests access, he or she shall also specify the preferred form of access to his or her personal data as follows: - oral information; - written information; - a personal review of the documents in which they are contained; - submission of the data on paper or by electronic means.

Article 35.

/1/ The person requesting access may submit the application through an attorney.

/2/ The person shall fill in a power of attorney in a standard form approved by the controller.

/3/ The power of attorney shall be made in plain written form and shall have the following content: 1. Name, address and other data required for the controller to identify the authorized person.

2. It shall explicitly state: a/ the data of the person who is authorized to submit an application to TGSOFT Ltd for access; b/ for access to which data the person is authorized to submit an application to TGSOFT Ltd .

3. It shall be signed by the authorizing person and shall be dated.

/4/ The person submitting the application shall present an original power of attorney, which shall be kept by the controller.

/5/ Access to personal data is prohibited unless the application is accompanied by an original power of attorney.

Article 36.

/1/ Each person shall have a right of access to another person’s data in the Register of Counterparties, subject to the procedure in these Rules.

/2/ The person requesting access shall fill in an application for access in a standard form approved by the controller /Appendix No. 4/. In addition to the necessary content, the reason why access to another person’s data is requested must also be stated. The wording shall be made in a free format, indicating what rights the person derives from another person’s data and/or what obligations the person performs.

/3/ The person to whose data access is requested shall permit the access in writing. The permission shall contain the following attributes: name of the person, signature and date, which shall be personally affixed; the personal data to which access is granted and the names of the person to whom access is granted.

/4/ The controller must provide the requested access without the permission of the data holder in any of the following hypotheses:

1. The personal data are required for the protection of the life and health of their holder.

2. The holder's condition does not enable him or her to give written permission.

3. The personal data are required for research or statistical purposes and are provided anonymously.

4. The processing is necessary for the fulfillment of the legitimate interests of the controller or of a third party to whom the data are disclosed, except where the interests of the natural person to whom the data relate override those interests.

/5/ The person requesting the access proves the existence of the specific hypothesis by attaching to the application the relevant documents /hospital record, death certificate, certificate of heirs, etc./. Register of access, rectification, objection or erasure of personal data in the

Register of Counterparties

Article 37.

/1/ The register is a book (notebook) in which the individual pages are numbered, signed and stamped.

/2/ The Register of access, rectification, objection or erasure of personal data in the Register of Counterparties contains:

1. Column "Number and date" – the application is filed with a sequence number and date of receipt, and each application is entered with an incoming number, starting from one, without missing consecutive numbers.

2. Column "Name and signature of the applicant", consisting of two columns – the person who submits the application is indicated in the first column and the same person attests it by his or her own personal signature in the second column.

3. Column "Notification", consisting of two columns – the date on which the person should personally receive the information is entered in the first column and the person signs. Having exercised his or her right, the person signs in the second column.

4. Column "Refusal" states the date of its service and the fact of the service is attested.

Submission of the application

Article 38.

/1/ Applications for access, rectification, objection or erasure of personal data in the Register of Counterparties shall be submitted to TGSOFT Ltd and shall be filed by the following positions:

assistant junior specialist of human resources, junior specialist of human resources, specialist of human resources, team leader.

/2/ Each application shall be filed and given an incoming number, and shall be entered in a Register of access to personal data.

/3/ The applications shall be stored and placed in folders, separately from the other documents received by TGSOFT Ltd .

/4/ The applications shall be stored in a separate folder within the statutory time limits and after that they will be destroyed.

Obligation to notify

Article 39.

/1/ After the application is filed, the person shall be notified on which date to appear in order to receive information about the exercised right.

/2/ An employee, holding any of the following positions: assistant junior specialist of human resources, junior specialist of human resources, specialist of human resources, team leader shall notify the person of the date on which he or she is to receive information about the exercised right.

Assessment of the lawfulness of the application

Article 40.

/1/ After the application is filed in the Register, its admissibility and the lawfulness of the requested access shall be verified.

/2/ The controller shall:

1. verify if the application submitted meets the formal legal requirements/is completed in accordance with the form approved by the controller; is accompanied by a power of attorney, written permission, documents required to prove the reasonableness, etc./;

2. verify if the application submitted meets the substantive legal requirements;

/3/ The verifications and/or assessments referred to in the previous paragraph shall be performed by the following positions: assistant junior specialist of human resources, junior specialist of human resources, specialist of human resources, team leader.

Obligations of the controller

Article 41.

/1/ The controller must satisfy the person’s right when there are legal grounds to do so.

/2/ The controller may submit the requested data in another form in the following cases: 1. Compliance with the form requested by the applicant would result in the improper processing of the information. 2. There is no technical ability to comply with the requested form.

Technical difficulty in granting access

Article 42.

Within the meaning of the PDPA, a technical difficulty for the controller is any of the following hypotheses: 1. Provision of more than 2 copies of the requested documents; 2. Provision of the requested information by electronic means.

Refusal of requested access

Article 43.

/1/ In case that the Controller is not entitled to provide the requested information, the following positions: assistant junior specialist of human resources, junior specialist of human resources, specialist of human resources, team leader shall draw up a refusal in an approved standard form /Appendix No. 5/.

/2/ The refusal shall comply with the following requirements: it shall be in writing and shall contain the following attributes: which data; for what reason and on what legal grounds their provision or rectification is refused, or why the controller refuses to stop processing them or to erase them; the authority before which and the period within which the refusal may be appealed.

Service of notice /refusal/ or provision of information

Article 44.

/1/ Any notice or refusal to provide information shall be served personally on the applicant requesting access to personal data.

/2/ The notice or refusal shall be served by the following positions: assistant junior specialist of human resources, junior specialist of human resources, specialist of human resources, team leader, manager within 14 days of receipt of the application.

/3/ The notice /refusal/ shall be served in the following ways: 1. Against the applicant's signature in the register. 2. By mail, against an advice of delivery. /4/ Upon service, the number of the advice of delivery and the date marked on it shall be entered in the register in the Column "Notification" or "Refusal".

Appeal

Article 45.

In case of violation of the natural person's rights under the PDPA, the person shall have the legal opportunity: 1. to file a complaint with the Commission for Protection of Personal Data within one

year after finding out about the violation, but not later than five years after its commission; 2. to appeal against the actions of the controller before the respective administrative court or before the Supreme Administrative Court, subject to the general rules of jurisdiction.

SECTION XIV FINAL PROVISIONS

Article 46.

/1/ The Rules shall be effective from 1 May 2018 and after all the persons for whom they establish subjective rights and obligations have been acquainted with their content.

/2/ TGSOFT Ltd undertakes to bring these Internal Rules to the attention of all employees/contractors.

Article 47.

/1/ Copies of these Internal Rules shall be available to the employees of TGSOFT Ltd . APPENDIX No. 2 INFORMATION on the implementation 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, the Personal Data Protection Act and the regulations on its implementation, and the internal rules and policy of TGSOFT Ltd as a controller during and in connection with the performance of selection or other inquiry in pursuance of a contract with a contracting entity and for the purpose of future, possible establishment of an employment relationship between the contracting entity and the data subject. TGSOFT Ltd informs you that the data voluntarily provided for the purposes of the selection or other inquiry made as part of its lawful activity and/or under a contract, aiming at possible establishment of an employment relationship with the contracting entity are personal and are subject to special protection arrangements within the meaning of Regulation 2016/679 and the Personal Data Protection Act. The personal data voluntarily provided shall be collected, stored and processed only for the achievement of legally permitted purposes and for the fulfillment of the legitimate interests of the controller related to its activity of selection and/or other forms of lawful inquiry. With your explicit consent, TGSOFT Ltd shall process, store, use and archive the voluntarily provided personal data for a period of 3 years from the date of the consent, when there is no statutory period to regulate and guarantee their security and secrecy. TGSOFT Ltd informs and the persons whose personal data are provided agree that TGSOFT Ltd shall submit the personal data to state authorities and institutions, or third parties, when it has such an obligation by virtue of a law or if it is necessary for the implementation of your rights and legitimate interests as a participant in the selection for the purpose of future, possible establishment of an employment relationship. TGSOFT Ltd informs the persons whose data are provided that, subject to its internal rules, the persons have a right of access and a right to rectification of their personal data, a right their personal data to be erased, and are also entitled to object to the processing, provision and disclosure of their personal data for purposes other than those stated herein.

APPENDIX No. 4

To

…… Incoming No.....

APPLICATION

by .....

/first name and surname/

holder of identity card No.....

address.....

contact telephone.....

position.....in .....

/structure – Directorate, Department, Workshop, etc./

The application is submitted personally/by an authorized person.

/delete as appropriate/

The application is for access to personal data/ rectification of personal data/ objection to the processing of personal data/erasure of the data subject /delete as appropriate/

1. I hereby request the preparation /provision/ of:

Oral information

Written information

Review of the data in the personal dossier

Copy of ..... documents.

/Please specify the information you request by writing in detail the types of documents to which you wish access./

The personal data are necessary in order to serve before

.....

.....

/Please specify before which authority and for what purpose you need the personal data./

2. Please rectify the following personal data:

……..

……..

/Please specify the types of personal data that you wish to be rectified./

3. I object to the processing of the following personal data:

……..

……..

/Please specify the types of personal data to the processing of which you object. /

4. I want to be erased as a subject whose personal data you are processing.

Enclosure: .....

Date: ..... Applicant: .....

/The information below shall be completed by the official of the controller./

The person was personally/through an attorney notified by.....,

holding the position....., to appear on.....,

at....., in order to receive information about the exercised right.

Date: .....

Official: ..... Applicant: .....

On..... personally and

within the statutory period, information about the exercised right was provided as follows:

.....

.....

.....

Date: .....

Official: ..... Applicant: .....

APPENDIX No. 5

TO

.....

/Write the Applicant's names /

REFUSAL

Outgoing No. .....date.....

By: ....., UIC....., having its seat and registered office in

the city of ....., represented by.....

We would like to inform you that based on Application for ..... /

specify the type of right requested to be exercised / incoming No.....date....., on the

grounds of ..... of the PDPA and due to the following reasons:

.....

.....

/Write the arguments for the refused access/

We refuse to.....:

.....

We would like to inform you that the refusal may be appealed before the Commission

for Personal Data Protection within.....period.

Date: .....

Official: ..... Applicant: .....