DataExpert Services Kft.
H–4026 Debrecen, Vendég utca 84. 1/7.

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

Effective: 23th of May 2018

Dezső Karasszon **Zoltán Vasvári**

GENERAL PROVISIONS

§ 1 Introduction

The Company declares to perform data processing activities – by adopting the appropriate internal regulations, technical and organizational measures – in compliance with 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 referred to as the Regulation) under all circumstances, as well as Act CXII of 2011 on informational self-determination and freedom of information (hereinafter referred to as the Data Privacy Act).

§ 2 Purpose of this Policy

1. The purpose of this Policy is the determination of the internal regulations and establishment of the measures that ensure the compliance of the Company's data processing activities with the provisions of the Regulation and the Data Privacy Act.

2. The Policy further aims at providing confirmation that the Company acts in conformance to the Regulation and in particular the principles relating to processing of personal data (Article 5) set out therein.

§ 3 Scope of the Policy

(1) The scope of this Policy shall cover the processing of personal data belonging to natural persons by the Company.

(2) For the purpose of this Policy, private entrepreneurs, one-man companies, small-scale agricultural producers as clients, customers and suppliers shall be regarded to be natural persons.

(3) This Policy does not cover the processing of personal data which concerns legal persons, including the name and the form of the legal person and the contact details of the legal person. (GDPR (14))

§ 4 Terms and definitions

For the purpose of this Policy, relevant terms and definitions are provided in Article 4 of the Regulation. Accordingly, the key terms and expressions are indicated below:

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

2. **"processing"**: means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval,

consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

3. **“restriction of processing”**: means the marking of stored personal data with the aim of limiting their processing in the future;

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

5. **“pseudonymization”**: 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 organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

6. **“filing system”**: means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;

7. **“controller”**: means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

8. **“processor”**: means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

9. **“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;

10. **“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 authorized to process personal data;

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

12. **“personal data breach”**: means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

DATA SECURITY MEASURES

(1) In association with its data processing activities for all purposes and legal grounds, the Company has worked out the technical and organizational measures that are required for the enforcement of the requirements of the Regulation.

(2) The Processor shall protect data with reliance on appropriate measures against accidental or illegal destruction, loss, alteration, corruption, unauthorized public disclosure or unauthorized access.

(3) The Company qualifies and handles personal data as confidential information. Employees shall be subject to confidentiality obligation in relation to the processing of personal data to which the stipulations set forth in a separate appendix shall apply. Access to personal data shall be restricted by the Company by defining authority levels.

(4) The Company shall protect its IT systems with the use of firewalls, and provide them with antivirus protection operated as per a separate set of regulations.

(5) The Company shall perform electronic data processing and record-keeping by means of computerized programs that comply with the relevant data security requirements. The program ensures access to the data only as required for specific purposes, under controlled circumstances and for persons who need the data for the execution of their tasks.

(6) During the automated processing of personal data, the controlled and processor shall take further measures to ensure

a) the prevention of the unauthorized entry of data;

b) the prevention of the use of automated data processing systems by unauthorized persons, with the use of data transmission equipment;

c) the option to control and ascertain as to which organizations personal data have been or may be forwarded with the use of data transmission equipment;

d) the option to control and ascertain as to which personal data have been entered into data transmission equipment, when and by whom;

e) the restorability of the installed systems in the event of any operating failure, and

f) the proper reporting of any error that occurs in the course of automated data processing.

(6) For the protection of personal data, the Company shall provide for the control of incoming and outgoing electronic communication.

(7) Documents subject to work or processing in progress may be accessed only competent administrators, while HR, payroll, labour-related and other documents containing personal data shall be kept as safely locked up.

(8) Proper physical protection shall be afforded to data, data carriers and documents.

THE COMPANY'S DATA PROCESSING ACTIVITIES

The Company is involved in data processing with respect to the following activities:

- Data processing
- Market research and public opinion polling

Guarantee pertaining to data processing

(1) With respect to expertise, reliability and resources, the Company as a processor guarantees that it shall execute the technical and organizational measures ensuring the fulfillment of the requirements of the Regulation, including the safety of processing activities.

(2) In the course of its activities, the Processor shall cause persons authorized to have access to the personal data of data subjects to undertake confidentiality obligations – unless they are otherwise subject to appropriate, statutory confidentiality obligations – in relation to the personal data that have become known to them. The wording of the applicable Confidentiality Declaration has been provided in a separate appendix to this Policy.

(7) The Company is in possession of appropriate hardware and software tools, and commits itself to execute the technical and organizational measures that are suitable for the safeguarding of the legality of data processing and the protection of the rights of data subjects.

(8) The Company is in possession of the legal and technical facilities, conditions required for electronic contacts with public bodies.

(10) Our Company agrees to provide the controller acting as the client with all the information that is necessary for the confirmation of compliance with the legal requirements relating to the engagement of a processor.

Obligations and rights of the client (Controller)

1. The Controller has the right to check the performance of the contracted activities at the Processor.

2. The Controller shall carry the responsibility for the legality of the Controller's instructions connected with the contracted tasks, while the Processor is obliged to notify the Controller promptly of any conflict of the Processor's instructions or the execution thereof with the relevant legal regulations.

3. The Controller shall inform the natural persons in relation to the contracted data processing operations, and secure their consent in case it is required by law.

Obligations and rights of the our Company as the Processor

1. **Right to instruct:** In its activities, the Processor shall act solely on the basis of the Controller's written instructions.

2. **Confidentiality:** In the course of its activities, the Processor shall cause persons authorized to have access to the personal data of data subjects to undertake confidentiality obligations – unless they are otherwise subject to appropriate, statutory confidentiality obligations – in relation to the personal data that have become known to them.

3. **Data security:** Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk. The Processor shall take steps to ensure that any natural person acting under the authority of the Processor who has access to personal data does not process them except on instructions from the Controller, unless it is required to do so by Union or Member State law. The Processor shall ensure that solely authorized persons should have access to the stored data via internal systems or by way of direct access, and only in association with the purpose of processing. The Processor shall provide for the necessary, regular maintenance, development of the tools and devices used. The Processor shall install the device in which data are stored in locked premises provided with physical protection, and ensure proper physical protection. For the performance of the contracted tasks, the Processor shall rely on the services of persons having adequate knowledge and experience. The Processor shall further ensure the preparation of the engaged persons as regards to the data privacy legal requirements to be observed, its contracted obligations, as well as the purpose and form of data registration.

4. **Reliance on other processors:** The Processor agrees to rely on the services of any other processor solely in conformance to the associated conditions set out in the Regulation. In the framework of this Policy, the Controller shall give general authorization to the Processor for the engagement of other processors (subcontractors). Before the engagement of any other processor, the Processor shall inform the Controller in relation to the identity of the other processor, as well as the tasks planned to be carried out by the other processor. If in the light of this information the Controller has any objection to the engagement of the other processor, the Processor shall have the right to engage the other processor only if the conditions described in the objection are satisfied. Where the Processor engages another processor for carrying out specific processing activities on behalf of the Controller, the Processor is required to enter a written contract for the activities concerned, while the same data protection obligations as set out in the contract between the Controller and the Processor shall be imposed on that other processor, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of this Regulation. Where that other processor fails to fulfill its data protection obligations, the initial Processor shall remain fully liable to the Controller for the performance of that other processor's obligations.

5. **Cooperation with the Controller:**

a) Our Company as the Processor shall assist the Controller in the facilitation of the enforcement of the data subjects' rights and the fulfillment of its associated obligations by all appropriate means.

b) Our Company as the Processor shall assist the Controller in ensuring compliance with the obligations pursuant to Article 32 to 36 (Data security, Data protection impact assessment and Prior consultation) taking into account the nature of processing and the information available to the Processor.

c) Our Company as the Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the Regulation (Processor), and allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller. With regard to this provision, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions.

The Company's general terms and conditions of contracting for data processing activities

(1) The Company shall enter into a written contract with the client for data processing activities.

(2) The Company's general terms and conditions of contracting for data processing activities are provided in a separate appendix to this Policy.

(3) The contents and substances of the general terms and conditions shall be presented to the other party, and whose consent thereto shall be secured prior to the conclusion of the contract.

MANAGEMENT OF PERSONAL DATA BREACHES

Definition of person data breaches

(1) "Personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed; (Article 4 of Section 12 of the Regulation)

(2) The most common reported breaches include – for instance – the loss of a notebook or mobile telephone, insecure storage of personal data (e.g. payroll documents thrown out to waste bins); insecure forwarding of data, unauthorized copying, forwarding of client and customer lists, server attacks, website hacking.

Management, rectification of personal data breaches

(1) The prevention, management of personal data breaches, the enforcement of the relevant legal requirements shall be the responsibility of the Company's manager.

(2) Successful and attempted accesses to IT systems shall be logged, and analyzed in an ongoing manner.

(3) If the Company's employees with controlling powers detect any personal data breach during the performance of their tasks, they shall promptly notify the Company's manager accordingly.

(4) The Company's employees are obliged to report to the Company's manager or the person exercising employer's rights in case any personal data breach or event involving the suspicion thereof has been detected.

(5) Personal data breaches may be reported via the Company's central e-mail address, telephone at which the employees, contracted partners, data subjects are enabled to report the underlying events, security weaknesses.

(6) When a personal data breach is reported, with the involvement of the IT, finance and operations manager, the Company's manager shall instantly investigate the report in order to identify the breach, and decide whether it is an actual breach or false alert. The following details shall be investigated and determined:

a. time, date and place of the occurrence of the breach,

b. description, circumstances, impacts of the breach,

c. scope, volume of data compromised during the breach,

d. scope of persons affected by the compromised data,

e. description of the measures taken for the counteraction of the breach,

e. description of the measures taken for the prevention, elimination, mitigation of damage,

(7) Upon the occurrence of any personal data breach, the affected systems, persons and data shall be defined and segregated, and provisions shall be made for the collection and retention of evidence supporting the occurrence of the breach. Thereafter, damager restoration may be commenced alongside the restitution of legal operations.

(8) Upon its occurrence, the personal data breach shall be reported to the supervisory authority without undue delay and not later than 72 hours, unless the Company is able to demonstrate that the personal data breach does not result in a risk to the rights and freedoms of natural persons.

Record-keeping of personal data breaches

(1) Proper records shall be kept of personal data breaches, including the following details:

a) scope of the personal data concerned,

b) scope and number of persons affected by the personal data breach,

c) time and date of the personal data breach,

d) circumstances, impacts of the personal data breach,

e) measures taken for the rectification of the personal data breach,

f) other information described in the legal regulation governing data processing.

(2) Information kept in the records of personal data breaches shall be retained for 5 years.