PRIVACY AND DATA PROCESSING POLICY

FROM STREETS TO HOMES ASSOCIATION

2020

Name of organisation: – Hereinafter ‘Data Controller’, ‘Controller’	**From Streets to Homes Association**
Headquarters:	112 Baross utca, Budapest 1082
Fiscal code:	18625880-1-42
Authorized representative:	Anna Bende co-President Vera Kovács co-President

These Rules should be revised and curated annually in connection to updated legal references.

Date of entering into force: 1 January 2020

Date of application: as of 1 January 2020

TABLE OF CONTENTS

I PURPOSE OF THE POLICY

The purpose of this policy is to set the internal regulations of the Data Controller's policy concerning data protection, data processing policy, the assurance of the respect for the privacy of natural persons in accordance with Act CXII of 2011 on Informational Self-Determination and Freedom of Information and with the data protection and data management provisions defined in REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (27 April 2016) on the protection of natural persons with regard to the processing of personal data, on the free movement of such data and on repealing Directive 95/46/EC – General Data Protection Regulation –, given that by enforcing these regulations the Data Controller could guarantee the right to protection of personal data during every activity and service delivery especially during data processing and controlling.
The Data Controller hereby declares compliance with the principles regarding personal data controlling as stipulated by Article 5 of REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND THE COUNCIL (hereinafter 'Regulation')

II SCOPE OF POLICY

1 Scope ratione personae

In terms of personal scope, this Policy applies to the Data Controller and those natural persons who are involved with data controlling activities. Data controlling activities stipulated in this Policy are directed at the personal data of natural persons. This Policy shall not cover personal data controlling of legal persons, or enterprises created as legal entities, including the name and form of such legal entities and the contact information of legal entities. Legal entities are associations, business organisations, cooperatives, professional associations and foundations.

2 DURATION

The duration of this Policy applies from the date of its establishment or until the day of its withdrawal.

III DEFINITIONS

1 ***subject:*** any individual person who can be identified via personal data
1(a) ***identifiable individual:*** Any individual person who can be identified, directly or indirectly, especially via an identifier such as name, on-line identifier, physical, physiological, genetic, intellectual, economic, cultural or social identity or via multiple identifiers;

2 ***personal data****:* any information relating to a data subject;

3 ***special category data:*** any personal data relating to race, ethnicity, political orientation, religious or philosophical belief, trade union membership in addition to genetic and biometric data for the unique identification of natural persons, health data and personal data relating to the sexual or sexual orientation of natural persons.
3(a) ***genetic data:*** personal data relating to the inherited or acquired genetic characteristics of a natural person and carrying special information concerning the data subject's physiological and health status resulting primarily from the analysis of a biological sample;
3(b) ***biometric data:*** any personal data about the data subject's physical, physiological or behavioural characteristics acquired via special procedures allowing the unique identification or authentication of a natural person such as facial image or dactyloscopic data;

3(c) ***health data:*** any personal data relating to the natural person's somatic, intellectual or health status, including data of health procedures provided for the natural person containing information about the health status of the natural person;

4 ***consent:*** any freely given, definitive and informed indication or expressive behaviour of the data subject's wishes by which he or she explicitly declares his or her consent to management of his or her personal data;

5 ***the concept of data controller:*** any natural or legal person (including organisations without legal personality) who (in the framework of acts and policies adopted by the European Union) alone or jointly with others determines the purposes of the processing of data, makes decisions regarding data processing (including the means) and implements such decisions itself or engages a data processor to execute them;
5(a) ***concept of joint data controller:*** data processor shall mean anyone who (in the framework of acts and policies adopted by the European Union) determines the purposes (and means) of the processing of data, and who alone or jointly with one or more other data controllers makes the decisions regarding data processing (including its means) and executes such decisions or engages a data processor to execute them;

6 ***data controlling:*** regardless of the method used, it is any operation or set of operations which is performed on the data (in particular collecting, recording, organization, storing, altering, using, retrieving, transmitting, disclosing, coordinating or combining, blocking, deleting or destroying, as well as preventing further use of the data, photographing, sound and video recording, and the recording of physical attributes for identification purposes such as fingerprints and palm prints, DNA samples and retinal images);

7 ***data transmission:*** the process of providing access to the data for third parties;
7(a) ***indirect data transmission*****:**
transfers of personal data from the third country or international organisation to controllers, processors in third country or international organisation via personal data transmission from the third country or international organisation to controllers, processors in third country or international organisation

8 ***public disclosure:*** the act of providing access the data for anyone;

9 ***data deletion:*** making the data unrecognisable in such a way that recovery is no longer possible

10 ***restriction of data controlling*****:** blocking of data stored in order to restrict further processing;

11 ***data destruction:*** the complete physical destruction of the data carrier;

12 ***data processing:*** the set of operations performed by the Data Processor on behalf of the Data Controller or based on the Data Controller's instructions;

13 ***data processor:*** any natural or legal person or entity without legal personality which (within the framework of acts and the policies adopted by the European Union) processes personal data on behalf of the Data Controller of based on the Data Controller's instructions;

14 ***data set:*** collection of sets of data in one register;

15 ***third party:*** any natural or legal person or organisations without legal entities 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;

16 ***personal data breach:*** 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;

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

18 ***recipient:*** a natural or legal person or an organisation without legal entity to which the personal data are disclosed by the Data Controller or the data processor;

19 ***pseudonymisation*** 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;

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

21 ***regulation:*** REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (27 April 2016)

22 ***data management system:*** tool used for data processing.

IV PRINCIPLES

(1) Personal data ought to be processed solely for a defined purpose in order to exercise a right or to fulfil an obligation.
(2) Data processing should be in accordance with the purpose of data controlling throughout the whole process; data recording and data processing should be fair and lawful. The personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed.
(3) It ought to be ensured that the period for which the personal data are stored (to the extent necessary) is limited to a time period until which the purposes are met.
(4) The Data Controller declares that the paper versions of the data processed can be found in the following location:

– headquarters: **112 Baross utca, Budapest 1082**
– other: rented office space at **46-48 Orczy út Budapest 1089**

(5) Methods of controlling personal data in the form of electronic data sets:
– Server hosted by the Data Controller
– Hard disk of (a) computer(s) belonging to the Data Controller's work organisation
– Cloud service used by the Data Controller Google Suite

(6) Personal data are processed by the Data Controller in compliance with legal requirements regarding data security.

(7) Provisions of paragraphs (4) and (5) cover any data controlling or data processing activities.

V LEGAL BASIS FOR THE PROCESSING OF THE DATA

1 Consent of the data subject

(1) Controlling of personal data ought to be lawful and based on the consent of the data subject or it needs to have a legal basis laid down by the law.
(2) The data subject can give consent to processing of his or her personal data in the following ways:

a) written statement in which he or she consents to processing personal data,
b) electronic consent by expressing explicit behaviour on the web page of the Controller, by ticking a box, by choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data.

(3) Silence, pre-ticked boxes or inactivity should not therefore constitute consent. (4) Consent should cover all processing activities carried out for the same purpose or purposes.
(5) When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.
(6) The data subject has the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent. The duration of data controlling, when based on the data subject's consent, lasts until the purposes for data controlling are met or until withdrawal of consent or until the execution of the decision of the court or authority to have the data deleted.

2 Performance of the contract

(1) Data controlling is considered lawful, when it is necessary for the performance of a contract where one of the parties is the data subject, or when it is necessary in order to honour the request of the data subject prior to entering into a contract.
(2) A consent from the data subject to control personal data that are unnecessary for the performance of the contract cannot be a requirement for the conclusion of contract.

3 Compliance with a legal obligation to which the controller is subject, or the protection of the vital interests of other natural person

(1) The legal basis for processing of data regarding the performance of a legal obligation is provided by the law, hence no consent by the data subjects is needed to control his or her data.
(2) The Data Controller is obliged to inform the data subject of the purpose, legal basis, duration of the date controlling, along with the identity of the data processor and legal remedies available.
(3) In the case the data subject withdraws his or her consent, the Data Controller is entitled to process those sets of data that are necessary so that the Data Controller could fulfil a legal obligation.

4 Performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, or for the purposes of the legitimate interests pursued by a controller or by a third party

(1) The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller. Such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller.
(2) At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place.
(3) The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing.

VI RIGHT OF ACCESS TO THE DATA

(1) Personal data can be accessed by:
– employee of the Data Controller entitled to have access to the data
– people or organisations performing data processing activities for the Data Controller (to the extent defined by the Data Controller)

(2) The data processors are as follows:

A) Name (Business Name): Beáta Mikle sole proprietor
Contact: mikle.bea@upcmail.hu
Name of authorised representative: Beáta Mikle
TEÁOR activity classification
6920 Accounting activities

B) Name (Business name): Ritecz János Péter sole proprietor
Contact ritecz.peter@utcárollakasba.hu
Name of authorised representative: Péter János Ritecz
TEÁOR activity classification
7022 Economic and Financial Affairs Activity

C) Name (Business name): Dóra Papadopulosz sole proprietor
Contact: papadopulosz.dora@utcárollakasba.hu
Name of authorised representative: Dóra Papadopulos:
TEÁOR activity classification
7021 PR, communications

C) Name (Business name) Zsuzsanna Máté sole proprietor
Contact mate.zsuzsanna@utcárollakasba.hu
Name of authorised representative: Zsuzsanna Máté
TEÁOR activity classification:
8899 Other social work activities without accommodation n.e.c.

VII. RIGHTS OF THE DATA SUBJECTS

1. Right to information

(1) Prior to the start of processing his or her data, the data subjects is entitled to be acquainted with the information related to date controlling.
(2) Information to be provided where personal data are collected from the data subject:

a) the identity and the contact details of the controller and, if any, of the controller's representative;
b) the contact details of the data protection officer, where applicable;
c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;
e) the recipients or categories of recipients of the personal data, if any;
f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

(3) In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or, where applicable, the right to object to processing or the right to data portability;
c) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
d) the right to lodge a complaint with a supervisory authority
e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;
f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

(4) Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information:

a) the identity and the contact details of the controller and, if any, of the controller's representative;
b) the contact details of the data protection officer, where applicable;

c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
d) the categories of personal data concerned;
e) the recipients or categories of recipients of the personal data, if any;
f) where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available.

(5) In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject:

a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
b) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;
c) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
d) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
e) the right to lodge a complaint with a supervisory authority;
f) from which source the personal data originate, and if applicable, whether it came from publicly accessible sources; and
g) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

(6) Where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

(7) Paragraphs 1 to 3 shall not apply where and insofar as:

a) the data subject already has the information
b) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;
c) obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; or

d) where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.

2. **Right of access by data subject**

(1) The data subject has the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

a) the purposes of the processing;
b) the categories of personal data concerned;
c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations
d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
f) the right to lodge a complaint with a supervisory authority;
g) where the personal data are not collected from the data subject, any available information as to their source;
h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

(2) Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.
(3) The Data Controller makes a copy of the personal data concerned available to the data subject. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form, unless the data subject requests otherwise.

3. Data subjects' right of rectification, and erasure
3.1. Right to rectification

(1) The data subject has the right to obtain from the controller without undue delay the rectification of inaccurate personal 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.
(2) For the right to rectification to be exercised, should the Data Controller or the data processor acting on his or her behalf find imprecise, false or missing data, then he or she rectifies or corrects them (especially when requested by the data subject); should it be in accordance with the purposes of data controlling, then the Data Controller amends the problem via personal data at his or her disposal or via a declaration made in connection to the personal data processed.
(3) The obligation of the Data Controller set out in Paragraph II shall be waived if

3.2. Right to erasure („right to be forgotten”)

(1) The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;
c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);
d) the personal data have been unlawfully processed;
e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

(2) Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

(3) Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

a) for exercising the right of freedom of expression and information;
b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);
d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
e) for the establishment, exercise or defence of legal claims.

4 Right to restriction of processing

(1) The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:

a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;
b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims; or
d) the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.

(2) Where processing has been restricted under paragraph 1, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment,

exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

(3) A data subject who has obtained restriction of processing pursuant to paragraph 1 shall be informed by the controller before the restriction of processing is lifted.

5 Notification obligation regarding rectification or erasure of personal data or restriction of processing

(1) The controller communicates any rectification or erasure to each recipient to whom the data have been disclosed, unless this proves impossible or involves a disproportionate effort.

(2) The Data Controller informs the data subjects of the recipients when requested.

6 Right to data portability

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

a) the processing is based on consent pursuant to point (a) (data subject's consent to the processing of his or her personal data) of Article 6(1) of the Data Protection Regulation or point (a) (data subject's explicit consent to the processing of his or her personal data) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and
b) the processing is carried out by automated means.

(2) In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.
(3) The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
(4) The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.

7 Right to object

(1) 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 carried out in the public interest or in the exercise of official authority; this objection is based on point (e) or (f) of Article 6(1) and it includes the right of objection to profiling based on the aforementioned provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

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

(3) Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

(4) At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.

(5) In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the data subject may exercise his or her right to object by automated means using technical specifications.

(6) Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1), the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

8 Right to exemption from automated decision-making

(1) The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.
(2) Paragraph 1 shall not apply where the decision:

a) is necessary for entering into, or performance of, a contract between the data subject and the controller
b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests
c) is based on the data subject's explicit consent.

(3) In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.
(4) Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

9. Right to complaint and legal remedy

9.1. Right to lodge a complaint with a supervisory authority

(1) The data subject shall have the right to lodge a complaint with a supervisory authority based on Article 77 of the regulation, should the data subject consider that the processing of personal data relating to him or her infringes this Regulation.

(2) Right to lodge a complaint with a supervisory authority can be exercised by contacting:

National Authority for Data Protection, address: 9-11 Falk Miksa utca Budapest 1055, telephone: +36 (1) 391-1400; fax: +36 (1) 391-1410 www: http://www.naih.hu e-mail: ugyfelszolgalat@naih.hu

(3) The supervisory authority with which the complaint has been lodged shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy pursuant to Article 78.

9.2 Right to an effective judicial remedy against a supervisory authority

(1) Without prejudice to any other administrative or non-judicial remedy, each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.

(2) Without prejudice to any other administrative or non-judicial remedy, each data subject shall have the right to a an effective judicial remedy where the supervisory authority which is competent pursuant to Articles 55 and 56 does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint lodged pursuant to Article 77.

(3) Member States shall provide for proceedings against a supervisory authority to be brought before the courts of the Member State where the supervisory authority is established.

(4) Where proceedings are brought against a decision of a supervisory authority which was preceded by an opinion or a decision of the Board in the consistency mechanism, the supervisory authority shall forward that opinion or decision to the court.

9.3. Right to an effective judicial remedy against a controller or processor.

(1) Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation.

(2) Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers.

10 Restrictions

(1) Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:

a) national security;
b) national defence;
c) public security;
d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;
e) other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation a matters, public health and social security;
f) the protection of judicial independence and judicial proceedings;
g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;
h) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g);

i) the protection of the data subject or the rights and freedoms of others;
j) the enforcement of civil law claims.

(2) In particular, any legislative measure referred to in paragraph 1 shall contain specific provisions at least, where relevant, as to:

a) the purposes of the processing or categories of processing,
b) a description of the categories of data subjects and of the categories of personal data,
c) the scope of the restrictions introduced,
d) the safeguards to prevent abuse or unlawful access or transfer,
e) the specification of the controller or categories of controllers,
f) the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing,
g) the risks to the rights and freedoms of data subjects; and
h) the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.

11 Information on the data protection incident

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

(2) The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the identity and contact details of the data protection officer or other contact point where more information can be obtained, the likely consequences of the personal data breach and 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.

(3) The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:

a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;
c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

(4) If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met.

VIII PROCEDURE TO BE APPLIED IN THE EVENT OF THE REQUEST OF THE PEOPLE CONCERNED

(1) The Data Controller aids the data subject in exercising his or her rights; the Data Controller shall not deny the execution of the request made to exercise the rights stipulated by this Policy, unless it is impossible for the Data Controller to identify the data subject.

(2) The controller shall provide information on action taken on a request to the data subject without undue delay, within 25 days (at maximum) of receipt of the request.

(3) Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

(4) If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

(5) Information provided under Articles 13 and 14 (under article 1 chapter VI of this Policy) and any communication and any actions taken under Articles 15 to 22 and 34 (feedback on the management of personal data, access of data processed, rectification, completion and erasure of personal data, restriction of the processing, data portability, objection against data processing, communication of a personal data breach) shall be provided free of charge.

(6) Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller 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 act on the request.

(7) Fee of charge: HUF 5000

(8) Fees for any additional copies of health data and personal data connected to them are to be paid as established by decree of the Minister. (Section (3) of Paragraph 7 of Act 47 of 1997)

(9) The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

(10) Without prejudice to Article 11, where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 15 to 21, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

(11) Should the Data Controller or the data processor acting on his or her behalf refuses the data subject's request concerning the rectification, erasure or restriction or the data at the disposal of the Data Controller, he or she would inform the data subjects without delay in writing of

a) the fact of rejection, its legal and factual grounds, and

b) the rights the data subject possesses based on this Regulation, and about the ways how he or she can enact these rights, hence especially of the right to of rectification, erasure or restriction of the processing of personal data available to the Data Controller (or the data processor acting on his or her behalf) could be exercised by the assistance of an authority.

(12) Should the Data Controller rectify, erase or restrict personal data managed by him or her or by someone on his or her behalf, the Data Controller shall inform the data controllers and the data processors of this measure, to whom the Data Controller forwards these data prior to these measures so that they could perform the rectification, erasure or restriction of personal data themselves during their data processing.

(13) For the purpose of enforcing the right to erasure, the Data Controller shall forthwith delete the relevant data of the data subject, if

a) data controlling proves to be illegal, especially if the data controlling

- goes against the principles of this present Policy

- loses its purpose or processing of given personal data is no longer relevant in order to reach the purpose of data collecting

- lapses at the end of the period stipulated by law, international treaties, a legally binding act of the European Union,

- loses its legal basis and these is no other legal basis for controlling the data,

b) the data subject withdraws his or her consent to data controlling or requests the deletion of his or her personal data (except for personal data being controlled based on legal authorities or when processing is necessary in order to protect the vital interests of the data subject)

c) a legal act of the European Union, an order of the court or an authority stipulates the erasure of personal data, or

d) the duration of the legitimate interest for not deleting the data subject's data has expired; or, in the case of international transmission, the duration of data retention of documentation duties has expired.

IX PROCEDURE TO BE APPLIED IN THE EVENT OF PERSONAL DATA BREACH

(1) Personal data breach under the Regulation is a breach of security which results in the destruction, loss, modification, unauthorised disclosure or the unauthorised access of transferred, stored data or data otherwise processed.

(2) Loss or theft of tools containing personal data (laptop or mobile phone) also qualify as a personal data breach, just like the loss or inaccessibility of code used by the Data Controller for decryption; ransomware (extortion attack) making data processed by the Data Controller inaccessible until a ransom is made is also considered to be a personal data breach along with, among others, an attack against the IT system, an e-mail containing personal data sent incorrectly or the disclosure of an address list.

(3) In case of a personal data breach, the Data Controller performs an investigation without delay in order to identify the personal data breach and its possible consequences. In order to remedy the damage, the necessary measures must be taken.

(4) Personal data breach must be reported without delay, if possible within 72 hours at maximum following learning about the breach, to the competent authority, unless the personal data breach does not seem to pose a threat to the rights and liberties of the natural persons involved. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

(5) The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

(6) The notification referred to in paragraph 1 shall at least:

a) describe the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
c) describe the likely consequences of the personal data breach;
d) 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.

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

(8) The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

X DATA PROCESSING ACTIVITIES OF THE DATA CONTROLLER IN RELATION TO EMPLOYMENT

1 Data controlling prior to the establishment of employment relationship

Data controlling prior to employment materialises via a recruitment process and a job aptitude test.

1.1 Data controlling during recruitment

(1) Data controlling during the recruitment process is authorised by the consent of the subject involved.

(2) Purposes of data controlling: evaluation of applications and concluding of employment contracts.

(3) Personal data involved during data controlling: name, address, place of birth, date of birth, education, professional qualifications, telephone number, e-mail address, picture,

(4) Categories of people involved in the data controlling: people applying for the job

(5) Recipients of personal data: the person exercising the employer's rights, employee(s) performing human resources tasks.

(6) Duration of data controlling: following employee selection, the purpose of data controlling ceases to apply regarding the unselected applicants, hence the personal data the unselected applicants are to be forthwith deleted.

(7) The obligation of deletion applies in those cases as well, when the applicant changes his or her mind during the recruitment process and withdraws his or her application. Applicants ought to be informed of the decision made concerning the recruitment process.

1.2. *Data controlling during job aptitude test*

(1) According to the Labour Code, only two types of job aptitude tests are to be used: aptitude test prescribed by terms and conditions governing the employment relationship, or a test not required by terms and conditions of employment, but which are necessary because of the exercise of right stipulated by regulations of employment or the performance of obligations. (Labour Code 10 § (4))

(2) Data subjects are to be informed in writing prior to either type of aptitude tests of data controlling, and among others, of what sort of competencies and abilities are assessed and with what sort of tools and methods. Should the test be required by law, employees are to be informed of the title of the legislation and of its exact provision as well.

(3) The employer’s legitimate interest serves as the legal basis for data controlling.

(4) Purpose of processing: determination of suitability for the position, conclusion of employment.

(5) People authorised to have access to personal data regarding the assessments are the professional performing the assessment and the subject assessed. The employer receives information about whether the person assessed is fit for work or not, and about what conditions need to be met for employment. The full documentation of the assessment shall not be disclosed to the employer.

(6) Duration of data controlling of personal data regarding aptitude tests: 3 years following the termination of the employment relationship.

2. **Data controlling throughout the duration of employment**

2.1.Data controlling while managing employment records

(1) The Data Controller processes the personal data listed below in a labour register, in accordance with the legitimate interest of the employer, fulfilment of legal obligations and the performance of the contract. Before the start of any data processing activity, the Data Controller informs the employee of the legal basis and purpose of the data controlling.

(2) Scope of personal data of employees controlled in the labour records:

a) name
b) address, temporary address, postal address
c) contact information, telephone number, e-mail address
d) social security number, fiscal code, identity card number,
e) salary,
f) bank account number,
g) attachments, deductions and the connected bank account numbers,
h) number of children or dependants along with their social security numbers,
i) next of kin.

(3) The persons involved in data processing: Data Controller and his or her employees.

(4) Recipients of personal data recorded: person exercising the Employer's rights, employees, data processors performing personnel management duties and accounting and payroll tasks.

(5) The purpose of the processing: performing duties resulting from an employment (pay) and exercising rights relating to employment. Establishment and termination of employment.

(6) Duration of data controlled: 3 years of the termination of the contract. (The deadline of erasure of data used for the fulfilment of tax and contribution obligations concerning is 8 years following the termination of the contract.) The storage period of employment documents relating to lengths of service, income and earnings used for the calculation of pension benefits is 5 year for the insured or ex-insured following pensionable age. (Section 99/A of Act 81 of 1997)

2.2 Data controlling aimed at monitoring employment behaviour

(1) Employees can only be monitored by the employer in connection with employment. The tools and methods used for these monitorings must not involve a violation of human dignity. The private life of the employee shall not be monitored.

(2) The employer informs beforehand the employee of the technological tools and applications used for monitoring of employees.

2.2.1 Data controlling in relation to the e-mail address provided by the Data Controller to the employee

(1) Employees are provided with e-mail accounts by the Data Controller so that they could communicate with each other or so that they could exchange e-mails with clients, other people or organisations while representing the Data Controller.

(2) Employees must not use the aforementioned e-mail addresses for private use. The data contained in the e-mail address provided for the employee can be disclosed for the manager. The

manager is entitled to monitor the content of the employee's e-mail address every 6 months along with the correspondence of the employee.

(3) Prior to monitoring the e-mail address of the employee by the employer, the employee must be informed of the interests of the employer leading to this action.

(4) The employer needs to develop a monitoring system subject to the principle of gradation, in which the protection of personal data must be respected along with the principle of the limiting intrusion to the employee's private life to a minimum.

(5) As a general rule, when monitoring the use of the e-mail address, the presence of the employee shall be guaranteed.

(6) In order to have the e-mail address monitored, the employer needs to inform the employee in detail about the procedure. Information should be provided to the employer about: – what is the purpose of the monitoring of e-mail addresses and what interest of the employer resulted in the monitoring (naturally, prior to the monitoring itself, employees must be informed of the interest of employers leading to the monitoring procedure) – who is allowed to perform the monitoring process on behalf of the employers, – what rules (the principle of gradation) and what sort of procedure are to be expected during the monitoring process, – what rights and legal remedies do employees have regarding the monitoring of their e-mail addresses.

(7) The first step of monitoring is the examination of the subjects of e-mails followed by monitoring higher-level uses of the e-mail account.

(8) The employer is not entitled to examine the content of private e-mails stored in the e-mail account provided, not even when the employee has been informed of the monitoring process prior to the monitoring. The employee must be asked to delete his or her private e-mails; should he or she not comply or should he or she be unable to delete these personal data (due to his or her absence), the employer is entitled to delete these personal data during the monitoring process without delay, and at the same time, the employer is entitled to apply labour law sanctions against the employee given violating policy regarding the use of company e-mail account.

(9) Every two months, the employer must send a notification in the mailing system regarding the ban on using company e-mail accounts for personal correspondence.

(10) The legal basis of e-mail account monitoring by the employer is the legitimate interest of the employer; the purpose of such monitoring is the examination of the performance of the duties of employees and the monitoring of compliance with the ban on the use of business e-mails for private uses.

2.2.2 Monitoring the laptop, tablet or telephone made available to the employee

(1) Employees in certain occupations could be provided "business" laptops, tablets or telephones by the employers so that they could perform their duties.

(2) The employer forbids employees from using the above-mentioned tools for private use. In accordance with the rule above, it is forbidden to use the tools listed above for storing and managing personal data such as photos, passwords of personal accounts, identifiers, electronic mails, private-use applications for personal use and to use them for conducting private conversations.

(3) Paragraph 2.2.1 describes the conditions that must be met while monitoring the aforementioned tools (personnel authorised to conduct the monitoring procedure, legal basis, purpose).

(4) Tools made available to employees:

– laptop,

– telephone.

2.2.3 Monitoring the internet use of the employee

(1) The employer does not allow personal internet use during work; employees are to use the world-wide web for work-related activities.

(2) Compliance with this policy is monitored according to Paragraph 2.2.1 which includes the labour law sanctions registered in that paragraph.

(3) Legal basis and purpose regarding the data controlling of the employee's internet use while at work are governed by Paragraph 2.2.1.

2.2.4 Ad hoc data controlling relating to employees

(1) The Data Controller organises team-building exercises and other events in order to enhance communication between employees, to enhance effective cooperation, trust in each other along with dedication and respect for one another; the Data Controller provides opportunities for employees to participate in these happenings.

(2) The legal basis for data controlling in connection with activities listed in paragraph 1 is the consent of the employee.

(3) The purpose of data controlling is to enhance communication between employees, to enhance effective cooperation, trust in each other along with dedication and respect for one another.

(4) The group of stakeholders involved: all those employees who participate in trainings and other events.

(5) Scope of personal data: image and voice of the employees.

(6) Deadline of deletion of data:

– 6 months following publication in the internal system of the employer.

(7) People authorised to access these data (categories of recipients): none

2.2.5 Specifications for the processing of biometric data of employees

(1) The Data Controller does not process biometric data of employees.

(2) In accordance with the provisions of the Labour Code, biometric data of the employees can only be used for identification when it is needed to prevent unauthorised access to data which would result in the grievous, massive and irreversible harm to

a) the lives, bodily integrity or health of employees or others

b) the prominent interest protected by law.

2.2.8 Rules relating to the controlling of personal criminal offences

(1) In accordance with the conditions defined in the Labour Code, the Data Controller processes criminal records only when accessing the Moral Certificate.

(2) Copying, storing, processing and forwarding criminal records is forbidden.

(3) The reason why the data Controller processes the criminal records of those intended to establish an employment relationship is because he or she examines whether the applicant is (by law or according to Paragraph 4) is under prohibition or restricted from a certain activity that would make his or her employment impossible.

(4) The Data Controller shall define limiting and disqualifying conditions according to Paragraph 3, if employment of the person involved would present harm to the following:

- substantial economic interest of the Data Controller
- secret protected by law
- defence of firearms, ammunitions, explosives, toxic or dangerous chemical or biological substances, nuclear materials or the defence of the defence worth at a minimum of HUF 50 million.

(5) The legal basis of data controlling is the legitimate interest of the Data Controller.

(6) The data processed while accessing the Moral Certificate: whether or not the employee has a criminal record.

(7) Categories of the recipients: the manager of the Data Controller as the person exercising the employer's rights, Head of Human Resources as the person making the decision on employment.

(8) The content of data controlling: after having accessed the Moral Certificate, the employer must give the certificate back to the employer. Data controlling shall have ceased by the time the employer has accessed the Moral Certificate. Data relating to the criminal record of the employee are not stored in the registry.

(9) The Data Controller registers in the Rules of Organisation a list of all those occupations that justifies the purpose of data controlling.

XI ADDITIONAL ACTIVITIES AND DATA SETS RELATING TO DATA CONTROLLING

1 Data management based on a legal obligation

1.1 Data controlling regarding data management based on an anti-money laundering obligation

(1) Based on paragraph 1 of article 6 of Act 53 of 2017 on Prevention of Money Laundering and the Financing of Terrorism the Data Controller is required to perform a customer screening of people representing natural persons, particularly upon establishment of business relations should the circumstances of money-laundering or the financing of terrorism emerge and should measures relating to customer due diligence not be enacted; such screening is also performed should any doubt arise concerning the validity of the customer identification data.

(2) During identification, the Data Controller must register the following personal data about the natural person acting in the customer’s name and on his or her behalf:

a) surname and first names
b) surname and first name at birth;
c) nationality;
d) place and date of birth;
e) mother’s maiden name;
f) address or lieu of it: place of residence;
g) type of identification document and its number.

(3) The scope of people involved during data controlling: people acting on behalf of clients or on the basis of a delegation of the client’s powers.

(4) Personal data remain accessible only to persons authorised to acquaint themselves therewith i.e. the manager appointed by the Data Controller to perform the customer due diligence or his or her employee. The Data Controller shall be entitled to manage personal data recorded during the customer due diligence procedure for 8 years from termination of the contract (business relationship).

(5) The person authorised to acquaint him- or herself with personal data shall make a copy of the documents containing the data of natural persons during the due diligence procedure in order to verify the customer's identity. The exception is the official address card's page containing the personal identification number, as no copies shall be made of it.

1.2 Data controlling to meet the accounting obligations

(1) The legal basis for the controlling of data of natural person clients, customers and suppliers of the Controller is [Section 1 of Paragraph 159 Act 127 of 2007 on value 159. added tax] while the purpose of processing these data is the determination of the obligatory content of invoices, issuing and maintaining receipts in accordance with Accounting Act [Section 2 of Paragraph 169 of Act 100 of 2000 169. on Accounting] or the performance of related accounting tasks.

(2) Scope of Data Subjects: natural person clients, customers and contractors of the Data Controller.

(3) Scope of personal data processed: names, addresses and fiscal codes of natural person clients, customers and contractors of the Data Controller

(4) Persons authorised to acquaint themselves with personal data are the manager, the employee and the manager designated to issue invoices. The Controller is entitled to manage data to fulfil the aforementioned legal obligations for 8 years following the termination of the contracts (business relationships).

1.3 Data controlling in relation to the fulfilment of tax and contribution obligations

In accordance with Section (1) of Paragraph 50 of Act 150 of 2017 on the Rules of Taxation, the Controller submits a declaration of fiscal and social security responsibilities arising from payments to individuals along with all taxes and contributions associated with benefits and/or data defined in paragraph 2.

(2) Scope of data subjects: manager of the Controller, his or her employees and family members.

(3) Scope of personal data processed: manager of the Data Controller, his or her employees and family numbers, data defined by Art. 50 of paragraph 2), especially the natural person identification details (including former name and title), sex, citizenship, fiscal code of natural person, social security number.

(4) Scope of recipients: employees of the Controller responsible for accounting and payroll activities and data processors.

(5) The Controller is entitled to manage personal data to fulfil legal obligations until 8 years following the termination of employment. Labour documents containing data relating to insurance and social security contributions shall not be culled.

1.4 Data controlling in relation to the obligation of taking out an insurance policy

(1) In accordance with No 3 of Annex I of Act 150 of 2017, when concluding an insurance contract, the employer is required to issue a declaration to the National Tax and Customs Administration.

(2) The scope of data subjects involved: the natural persons concluding insurance contracts (employment, contract agent relationship).

(3) Scope of personal data processed: surname and first name of insured persons, fiscal number, date of birth, start, code and end of insurance, interruption of insurance, weekly working time, FEOR (Hungarian Standard Classification of Occupations) number, social security number, education, vocational training, professional qualifications along with the names of the institutions issuing these documents and the qualification document number. Should the insured not have a fiscal code, it is necessary to include his or her natal surname and first name, date of birth, mother's maiden name along with his or her nationality when submitting the declaration.

(4) Scope of recipients: employees, data processors of the Controller responsible for accounting and payroll activities and data processors.

(5) Purpose of data controlling: compliance with legal obligations.

Duration of data controlling: 5 years following the end of status, except for employment documentation relating to contribution and insurance which cannot be discarded.

1.5 Data controlling in relation to handling complaints

(1) In order to promoting consumers' rights, the Controller informs the data subject of his or her headquarters, the place of complaint handling, the process of complaint handling and the mailing address of the customer service as stipulated by Section 1 Of Paragraph 17/A of Act 155 of 1997 .

(2) Data subjects involved: every natural person asserting rights as consumers against the Data Controller.

(3) Scope of personal data processed: name, address, place and date of complaint, mode and description of complaint, identification number of complaint.

(4) Scope of recipients: employees of the Data Controller responsible for customer service along with the manager of the Data Controller.

(5) Purpose of the processing: compliance with legal obligations.

(6) The Data Controller shall keep a statement concerning the complaint along with the copy of the answer for 5 years and submit it to the control authorities when requested (in compliance with Section 7 Of Paragraph 17/A of Act 155 of 1997).

2 Data controlling in relation to requests for information and requests for proposals

(1) Relating to services offered by the Controller and relating to products sold, the Controller offers third parties the opportunity for requests for information and for calls of proposals.

(2) The legal basis for requests of information and calls of proposals is the consent of the data subjects involved.

(3) The scope of data subjects involved in case of request of information and a call of proposal: every natural person requesting information concerning a service of product of the Data Controller, calling for a proposal, while providing personal data.

(4) Scope of personal data processed:

– name,
– address,
– telephone number,
– e-mail address.

(5) Purposes of data controlling in the case of requests of information: identification, communication.

(6) Purpose of data controlling in the case of a call of proposal: making an offer, communication.

(7) Recipients of data (those who can get access to the data) in case of requests of information and calls of proposals are the following: manager of the Data Controller and the customer responsible for customer service tasks.

(8) Duration of data controlling in the case of request of information and call of proposal: 30 days after providing information and making an offer, the Data Controller deletes all personal data.

3 Data controlling in relation to the websites operated by the Data Controller

3.1 Information relating to the data of visitors of the Data Controller's website

(1) If the person visiting the web page gives his or her (active) consent by continuing the browsing activity following information included in a clear and concise manner, then one or more cookies (small packages of information send from the server to the browser, then send back to the server from the browser during requests directed towards the server) are sent to the person visiting the website making the browser individually identifiable during these visits on the web page of the Data Controller. A person visiting the website may disable cookies in his or her browser.

(2) Cookies may only be set in order to enhance user experience and to automate the login process. Cookies used on the website do not store data that can be used to identify people, the Data Controller engages in no data controlling regarding this issue; only IP address, operation system, browser program, URL link of pages visited and date of visit are recorded.

(3) Concerning embedding plug-ins of social media on the website, the Data Controller provides the following information: given the embedded plug-ins, the Data Controller transfers user data to that particular social media (Facebook, Twitter, Pinterest, LinkedIn) whose plug-in has been embedded. User data transferred are defined in Paragraph 2. Following the transmission of data, it is the responsibility of the social media platform to provide information to the user relating to the management of incoming data.

3.2 Signing up to the newsletter

3.2.1 Signing up to the newsletter

(3) Legal basis for data controlling relating to subscription to the newsletter is the consent of the data subject which is given by checking the box next to the text "subscription to the newsletter" following information regarding data controlling.

(2) Scope of data subjects in the case of subscription to the newsletter: every natural person who signs up for the newsletter of the Data Controller, registers on the web-page and gives his or her consent to processing his or her personal data.

(3) Scope of data controlled in case of signing up to the newsletter:

– date of signing up
– name
– e-mail address

(4) Purpose of signing up to the newsletter: communication of services and products of the Controller to the data subject involved, and of news and events regarding changes in either of them.

(5) Recipients of data (those who can get access to the data) in the case of signing up to the newsletter: manager of the Controller, employee responsible for customer services, data processing employee responsible for the operation of the Data Controller's web page.

(6) Duration of data controlling regarding signing up to the newsletter: until the withdrawal of consent or unsubscribing from the newsletter.

(7) The data subject involved shall unsubscribe from the newsletter any time, what is more, he or she may request the erasure of his or her personal data. Unsubscribing is done by clicking on the link provided in the footer of electronic letters sent to the data subject or by a letter sent to the postal address of the Data Controller.

3.2.2 Registration

(1) The legal basis for data controlling is the consent of the data subject given checking a box next to the text "registration" following information about the management of his or her data.

(2) Scope of recipients in case of registration: every natural person who registers on the web-page of the Controller and gives his or her consent to the management of his or her personal data.

(3) Scope of data controlled in case of registration:

– date of registration
– name
– address
– e-mail address
– telephone number
– password
– other

(4) Purpose of data controlling in case of registration: contact for the preparation of contracts, providing services available on the site for free, providing access for the public content of the web site.

(5) Recipients of data (those who can get access to the data) in case of registration: manager of the Controller, employee responsible for customer services, data processing employee responsible for the operation of the Data Controller's website.

(6) Duration of data controlling in case of registration: until the withdrawal of consent.

(7) The data subject involved may request the deletion of his or her registration (personal data) any time. The deletion of registration may be initiated by the data subject involved sending an electronic letter to the e-mail of the Data Controller.

3.3 Data controlling relating to direct marketing activity via the website

(1) The legal basis of data controlling aimed at direct marketing is the clear and explicit consent of the data subject. Clear and explicit consent is given on the website of the Data Controller by checking the box next to the text describing the consent to direct marketing communications following information regarding data controlling.

(2) Scope of recipients: every natural person who has given his or her clear, explicit consent for the Data Controller to have his or her personal data processed for direct marketing purposes.

(3) Purposes of data controlling: identification, contact concerning services, messages containing ads regarding selling of products, sending of offers, information about actions via electronic means.

(4) Recipients of personal data: manager of the Controller, employees responsible for customer services and marketing tasks.

(6) Scope of personal data processed:

– name
– address
– telephone number
– e-mail address
– other

(6) Duration of data controlling: withdrawal of consent concerning the use of personal data for direct marketing purposes. (objection)

3.4 Data controlling relating to the web shop operated by the Data Controller

(1) The rules of procedures to be applied regarding registration to the web shop, subscription to the newsletter and visitor information are the provisions set in points 3.1, 3.2 and 3.3.

(2) On-line conclusion of contracts (purchases) on the web site of the Data Controller are subject to the Act 108 of 2001 (on Electronic Commerce and on Information), hence the purposes for data controlling besides the aforementioned are compliance with employer obligations, proof of conclusion of the contract, establishing a contract and setting its content, monitoring the performance of the contract, billing the fees in connection to the contracts and the enforcement of debt recovery.

(3) Legal basis for data controlling in case of purchase at the web shop is the performance of the contract along with fulfilling legal obligations.

(4) Categories of the data controlled:

– names of customer
– addresses of customers,
– telephone numbers of customers,
– login password of customers,
– bank account number of customers.
– other

(5) Categories of data subjects involved: every natural person who has registered to the web shop of the Data Controller, subscribed to his or her newsletter and has purchased something.

(6) Categories of recipients of personal data: manager of Data Controller, employee responsible for customer services and sales tasks, data processing employee responsible for the operation of the Data Controller's website, employees responsible for accounting tasks and employees responsible for these tasks.

(7) Location of data management is registered in Paragraph 4 of Section IV of the present document.

(8) Duration of data controlling: 5 years following the termination of contract.

3.5 Rules concerning the presence on social media

(1) The Data Controller is present on the following social media sites:

– Facebook
– Twitter
– Instagram
– YouTube

– Tumblr
– LinkedIn
– TikTok
– Other

(2) Categories of data subjects: natural persons who follow the social media pages of the Data Controller.

(3) Legal basis of data controlling regarding following the social media pages of the Data Controller: voluntary consent of the data subjects

(4) Categories of data controlled: The Data Controller does not manage data shared by users on social media platforms; the purpose of presence on social media is sharing and promotion of the Data Controller's products and services along with contact with those following the pages for the sake of the aforementioned matters. The Data Controller manages the name of the follower, but does not manage other data shared on social media by the followers; these data are subjected to the data processing policy of the respective social media sites.

(5) Categories of recipients of personal data: employee responsible for managing the social media platforms of the Data Controller, manager of the Data Controller.

(6) Duration of Data Controlling: until withdrawal of the data subject's consent.

4 Activity linked to the implementation of contract

(1) Data controlling of personal data of those natural persons (clients, customers, suppliers) who entered into a contract with the Data Controller are provided in the context of the contractual relationship. Data subjects must be informed of the personal data controlled.

(2) Scope of data subjects: every natural person who entered into a contract with the Data Controller, and the contacts of legal persons who are in contract with the Data Controller.

(3) Legal basis for the processing of data is the performance of contract; the purpose of the processing is communication, enforcement of contractual claims and ensuring compliance with substantial contractual obligations.

(4) Recipients of personal data: manager of the Data Controller, employers, data processors responsible for customer services and accounting tasks.

(5) Scope of personal data processed:

- name of private individual customer
- address of private individual customer
- telephone number of private individual customer
- e-mail address of private individual customer
- bank account number of private individual customer
- business license number
- primary producer license number
- name of contact of business organisation customer
- e-mail address of contact of business organisation customer
- telephone number of contacts of business organisation customer
- other

(6) Duration of data controlling: 5 years of the termination of the contract

4.1 Management of health data linked to the implementation of contracts.

(1) Health data of natural persons in contract with the Data Controller are managed in accordance with the applicable legal provisions.

(2) Scope of data subjects: every natural person who are in contract with the Data Controller and who give their voluntary and explicit consent to processing their health data regarding the performance of the contract following adequate information.

(3) Legal basis of data controlling: performance of the contract, consent of the data subject.

(4) Purpose of the processing: conclusion of contracts, compliance with the contractual terms, maintaining contracts, presenting a defence against legal claims arising from the contract following the termination of the contract.

(5) Recipients of personal data: manager of the Data Controller.

(6) Scope of personal data processed: data containing information regarding the past, present and future physical and mental health status of data subjects are only used when necessary to the performance of the contract, hence numbers, symbols or particulars assigned to a natural person to uniquely identify the natural person for health purposes and information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject.

(7) Duration of data controlling: 5 years of the termination of the contract.

5 Data controlling relating to prize competitions

(1) Occasional prize competitions organised by the Data Controller, the Data Controller is entitled to process the personal data of participants defined below given their consent, for the purpose of the declaration of the winner and for contacting the winner in order to present him or her with the price.

(2) Legal basis for data processing: consent of the data subject.

(3) Scope of data subjects involved: any natural person who participates in the prize competition organised by the Data Controller and who consents to processing their data for the above-mentioned purposes.
(4) Scope of personal data processed: name, date of birth, address, e-mail, telephone number.

(5) Recipients of personal data: employee responsible for the customer service tasks and the courier performing data processing tasks.

(6) Duration of data controlling: 30 days following the declaration of the results of the prize competition.

6 Data controlling relating to off-line direct marketing activity

(1) The legal basis of data controlling for the sake of direct marketing is the clear and explicit consent of the data subjects involved. Clear and explicit consent is to be given via filling in a form set out in Annex II of this Policy.
(3) Scope of data subjects involved: every natural person who gives his or her clear and explicit consent for the Data Controller to process their personal data for the sake of direct marketing.
(4) Purpose of data controlling: identification, contact concerning services, messages containing ads regarding selling of products, sending of offers, information about actions via electronic means.
(5) Recipients of personal data: manager of Data Controller, employees responsible for customer services and marketing tasks.

(6) Scope of personal data processed:

- name
- address
- telephone number
- e-mail address
- other

(7) Duration of data controlling: personal data are used for the purposes of direct marketing until revoked by the data subject, (objection)

XII RULES RELATING TO DATA PROCESSING

1 Rules relating to data processing

(1) As defined in Paragraph 2 of Section VI of the present Policy, the Data Controller may use the contribution of external data processor(s).

(2) Rights and obligations regarding data controlling of the data processor's personal data are subject to legal provisions along with the framework defined by the Data Controller in accordance with relevant legislature.

(3) The Data Controller declares that the data processor is not given competence to make a substantive decision regarding data controlling, personal data disclosed to him or her may only be used in accordance with the instructions of the Data Controller, he or she may not perform data processing for his or her own purposes; in addition to the aforementioned steps, he or she must store and preserve personal data in accordance with the instructions of the Data Controller.

(4) The legality of instructions given to data processors during the data controlling process is the responsibility of the Data Controller.

(5) It is the responsibility of the Data Controller to provide information for the data subjects involved about the identity of the data processor and the location of the data processing.

(6) The Data Controller gives permission for the data processor to use additional data processors.

(7) Contracts for data processing shall be in writing. No organisation may be commissioned to process data which has a financial interest in personal data which the Data Controller needs processed.

XIII PROVISIONS CONCERNING DATA SECURITY

1 Principles for implementing data security

(1) The Data Controller may only process data in accordance with the activities defined in this Policy.

(2) The Data Controller is responsible for the security of data and shall undertake to do every technical and organisational steps that are absolutely necessary in order to respect the legal provisions regarding data security along with data and confidentiality rules; what is more, the Data Controller develops the necessary procedure for the enforcement of the aforementioned legal provisions.

(3) Technical and organisational measures implemented by the Data Controller are aimed at:

a) the pseudonymisation and encryption of personal data;

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

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

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

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

(5) The Data Controller shall defend the data with appropriate procedures against unauthorised access, alteration, transfer, disclosure, erasure, or destruction along with accidental destruction, damage and inaccessibility arising from changes in the technology used. The Controller shall:

– deny unauthorised persons access to processing equipment used for processing (equipment access control);

– prevent the unauthorised reading, copying, modification or removal of data media (data media control);

– prevent the unauthorised reading, copying, modification or removal of data media (data media control);

– prevent the unauthorised inspection, copy, modification, or deletion of personal data while transferred or transported via a data carrier.

(6) Personal data processed by the Data Controller are managed in accordance with the legal provisions ensuring that they are disclosed merely to employees and those people acting on behalf of the Data Controller who need these data in order to perform their occupational tasks.

(7) The Data Controller stores personal data given during separate data processing activities separately, so that (in accordance with the aforementioned provisions) the respective data sets may only be accessible to employees with the appropriate access authorisation.

(8) Managers of the Data Controller along with their employees make the necessary steps to prevent unauthorized access to personal data. The Controller shall not transfer personal data

to third parties.

(9) The Data Controller grants access to personal data for those employees who, by making confidentiality statements, are subject to data security provisions and are required to meet these obligations. (The confidentiality statement is part of the clause of data protection contract present in Annex 14 to this Regulation)

The Controller shall ensure:

- that people granted access to the data processing system may process data exclusively defined by the access authorisation,

- that it is subsequently possible to verify and establish which personal data have been input into automated data-processing systems, when and by whom (input control)

- that it is possible to verify and establish to which bodies personal data have been or may be transmitted or made available using data communication equipment.

(10) The Data Controller, while establishing the provisions serving the protection of data, considers the current state of development of the technique; in the case of multiple suitable data processing

alternatives, he or she chooses the alternative with the highest level of personal data protection except for when presenting disproportionate difficulty.

2 Protection of the IT records of the Data Controller

(1) The Data Controller takes the following appropriate measures regarding the realisation of data security in the IT records:

a) provides protection against viruses for the data managed (by using real-time anti-virus software);

b) ensures the physical protection of the IT system's hardware (including defence against natural forces);

c) ensures protection against unauthorised access to the IT system regarding both software and hardware tools;

d) makes the necessary steps necessary to restore data sets, performs regular, security backups and provides for the separate and safe storage of the security backups.

(2) The Controller ensures that:

- in the event of a malfunction, the data management system be restored

- the data management system be operational with reports made of malfunctions arising during operations; what is more, the Controller needs to ensure that the personal data stored be unalterable by the malfunctioning of the system.

3 Protection of the paper records of the Data Controller

(1) The Data Controller makes the necessary provisions to protect paper-based records, especially with regard to physical security and fire protection.

(2) The manager of Data Controller his or her employees and other people acting on behalf of the Data Controller shall protect data carriers containing personal data in their protection/processed by them, independent of the method of recording; the aforementioned individuals must store them in safety and defend them against unauthorised access, modification, disclosure, erasure, eradication, accidental destruction or damage.

XIV ADDITIONAL PROVISIONS

(1) The executive of the Data Controllers needs to describe provisions set in this Policy for each employee of the Data Controller

(2) Data Protection Officer shall not be appointed.

(3) The executive of the Controller shall ensure that all employees of the Data Controller comply with provisions set in this Policy. In order to perform this duty, the executive of the Data Controller shall require the modification of the contracts between the Data Controller and his or her employees, so that they contain a declaration of obligations of compliance with and enforcement of this Policy.

(4) The Data Controller shall transfer data to the competent authorities at the request (for factual information, communication of data) of the authority; the request needs to show purpose, and the transfer needs to comply precisely with these purposes.

(5) In every three years at least, the Data Controller reviews whether the data controlling performed by the data processor authorised by him or herself or by the data processor acting on his or her behalf is enough for the purpose of data controlling. The Data Controller shall document the conditions and the results of this review and keep it for ten years should the National Authority for

Data Protection and Freedom of Information request the document to be disclosed to them.

(6) The executive of the Data Controller is responsible for the establishment and modification of this Policy.

Date: Budapest 01 JANUARY 2020

_____

Anna Bende