DATA PROCESSING POLICY

Publication of the current version: 25 May 2018

Identification data of the Enterprise, as the controller:	**Aliz Tech Kft.** **seat: 1143 Budapest, Gizella út 42-44.** **company Reg. No: 01-09-924920** **tax No: 14894413-2-42** **hello@aliz.ai** **https://aliz.ai/**
Name and contact data of the representative for the Enterprise, as the controller:	**István Boscha Executive Director**

Definitions, explanatory notes (see also Article 4 of the GDPR)

processor	a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller
processing	any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction
controller	the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law
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
recipient	a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in

	compliance with the applicable data protection rules according to the purposes of the processing
data concerning health	personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status
Data Subject	the natural person the personal data of whom is processed
consent of the Data Subject	any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her
EU member state	the member states of the European Union; currently Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Ireland, Italy, Latvia, Lithuania, Luxemburg, Hungary, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, and the United Kingdom
supervisory authority	an independent public authority which is established by a Member State pursuant to Article 51, in Hungary: the Hungarian National Authority for Data Protection and Freedom of Information (NAIH)
GDPR	REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
third party	a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data
sensitive data	personal data within the special categories of personal data
international organisation	an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries
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
personal data	any information relating to an identified or identifiable natural person (“data subject”); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

special categories of personal data	personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation
Enterprise	Hungary Kft., as controller

1 The objective of the Policy

The main objective of the Policy is the introduction and consistent application of provisions that ensure the accurate and safe handling of the personal data of Data Subjects, in accordance with the effective data protection rules of the European Union and the Member States, as well as with the Haldex Privacy Policy, implemented consistently at the level of the Enterprise.

At the same time, the Policy provides concise, transparent, and easily accessible information for Data Subjects about accessing their personal data controlled by the Enterprise; furthermore, it rules over and provides information about regulations on safeguarding the rights of Data Subjects by the Enterprise.

2 Fundamental principles of data processing

Before starting to process personal data, it shall be carefully assessed whether data processing is absolutely necessary. The processing of personal data shall only be initiated if it is justifiable beyond any doubt that the objective of data processing cannot be achieved in any other way (data minimisation).

The Enterprise is liable for the legitimate, honest, and transparent handling of the personal data of Data Subjects. No harm shall be caused to anyone by initiating a proceeding, an appeal, or filing an application at the Enterprise or any other authority determined in the present Policy, and, in case of data processing based on consent, by refusing to or withdrawing their consent ("harm" shall not include any incidental unfeasibility of a given legal obligation).

The collection of personal data of the Data Subjects shall only be carried out for a specified, explicit and legitimate reason (purpose limitation). The Enterprise is liable for a priori avoiding, or ultimately terminating any data processing carried out in a way not conforming to the objective regarding the given personal data. The Enterprise is entitled to control personal data only to the extent necessary, and is obliged to cancel all the personal data the processing objective of which is ceased, or in case the legal basis of data processing cannot be confirmed.

The Enterprise is liable for the introduction of monitoring mechanisms that are adequate for ensuring in advance, or subsequently as a way of supervision, that

(i) the personal data are consistent with the objectives of data processing at the time of data collection, and for the entire duration of processing; and

(ii) the extent of data processing is limited to the necessary minimum regarding the scope of data as well as the duration of processing.

The personal data controlled by the Enterprise shall be accurate and up-to-date. The Enterprise shall take all the reasonable actions in order to process accurate personal data,

(i) the personal data unnecessary for the objectives of the data processing, or the data which in the meantime has become unnecessary shall be cancelled without delay;

(ii) any inaccurate personal data shall be corrected or cancelled.

The personal data shall be kept in a way that the identification of the Data Subjects is only possible for the duration necessary for achieving the objectives of processing personal data.

The processing of personal data shall be exercised in a way that by the adequate technical and organisational measures, the necessary safety of personal data is ensured, including all the measures for the protection against any unauthorised or unlawful treatment, incidental loss, destruction or damage of personal data.

3 Lawfulness of processing

The appropriate definition of the basis for processing, and compliance with further conditions regarding the chosen legal basis are prerequisites for the lawfulness of processing. Therefore, in the strict sense, the requirement of lawfulness presumes the existence of an adequate legal basis for data processing; from a broader perspective, the processing of personal data may only be carried out in accordance with the legislation regarding the given legal basis for data processing.

The Enterprise, considering its activities carried out and regarding the personal data of Data Subjects, may choose from the following legal bases, in accordance with the nature and circumstances of processing. The main legal bases in the first subitem apply for all personal data except for the special categories of personal data, while the second subitem determines specific provisions regarding legal bases for special categories of personal data.

3.1 Personal data (except for "special", sensitive data)

The personal data, not including sensitive data of the Data Subject may be controlled by the Enterprise based on the following legal grounds:

(i) Consent: Data Subjects may give their consent for the control of their personal data, if the voluntary nature of the consent can be proved. The Data Subject provides their consent voluntarily, and is entitled to the withdrawal thereof at any time. The withdrawal does not affect the lawfulness of data processing carried out prior to the withdrawal; however, it may influence the sustainability of legal relationships requiring data processing.

(ii) Preparation and/or execution of a contract: to be applied in case of data processing necessary for the execution of a contract (e.g. service agreement, work contract, study contract), in which the Data Subject is one of the parties, or in case data processing is necessary for taking the actions at the request of the Data Subject prior to the conclusion of the contract.

(iii) Compliance with a legal obligation: data processing required by EU or national legislation.

(iv) Legitimate interest: includes data processing necessary for pursuing the legitimate interests of the Enterprise or a third party. The legitimate interests of the Enterprise or the third party are defined in the data processing notification regarding the given data processing objective. Data processing based on legitimate interest may only be executed in case the Enterprise conducts an interest assessment survey, in which it is described and examined whether the legitimate interest of the Enterprise proportionately limits the Data Subject's right to the protection of personal data, and privacy, and how the balance between the interests of the Enterprise and the Data Subject can be ensured. The interest assessment survey does not constitute a part of the data processing notification.

In case the Enterprise collects data from the Data Subject, but the Data Subject does not provide the data to be processed under the aforementioned legal grounds, a possible consequence of providing such data may be the refusal or unfeasibility of the preparation and execution of the given contract (e.g. failure to establish employment relationship). In case the Data Subject does not provide only a part of the data to be provided, it shall be decided based on the insufficiently provided data whether the failure to provide such data is the reason for e.g. the unfeasibility of the conclusion or maintenance of the contract. In case of

processing based on a contract, the legal consequences of unfeasibility may only be applied by the Enterprise if they certify that the execution of the contract concerned is impossible without the data to be provided.

3.2 Sensitive data

Due to the fundamental rights and freedoms of natural persons, sensitive data are special and high-risk data by nature, which require particular protection. The Enterprise may control the sensitive data of the Data Subject – primarily included are health data – in particular for the following objectives and under the following legal grounds:

(i) Article 9, paragraph (2), item a) of the GDPR: Data Subjects may give their consent for the control of their personal data, in case the voluntary nature of the consent can be proved. The Data Subject provides his or her consent voluntarily, and is entitled to the withdrawal thereof at any time, which does not affect the lawfulness of data processing carried out prior to the withdrawal.

(ii) Article 9, paragraph (2), item b) of the GDPR: in case of e.g. EU or Member State law and/or entitlement by a collective agreement under Member State law, the Enterprise may carry out data processing to execute their obligations regarding legislation on social safety and social protection, and to exercise their specific rights.

(iii) Article 9, paragraph (2), item f) of the GDPR: this legal basis is to be applied in case the control of sensitive data is necessary for the establishment, exercise or defence of legal claims (see also Article 9 of the GDPR).

4 The obligation to inform and the measures of the Enterprise

The Enterprise shall provide clear and comprehensible information to the Data Subject in a concise, transparent, and easily accessible way, and inform the Data Subject of the rights thereof (see also Article 6). Furthermore, the Enterprise may implement measures complying with certain procedural provisions for the request of the Data Subject.

4.1 Data processing notification

Depending on whether the Enterprise collects personal data from the Data Subjects themselves or not, the Enterprise is obliged to provide certain information for Data Subjects regarding data processing.

4.1.1 Common rules

Based on the obligation to inform, the Enterprise shall inform the Data Subject about the following:

(i) The identity and the contact details of the Enterprise and, where applicable, of the Enterprise's representative,

(ii) the contact details of the data protection officer,

(iii) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing,

(iv) where the processing is based on Article 6, paragraph (1), item f) of the GDPR, the legitimate interests pursued by the Enterprise or by a third party,

(v) the recipients or categories of recipients of the personal data, if any,

(vi) where applicable, the fact that the Enterprise 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 of the GDPR, or the second subparagraph of Article 49, paragraph (1) of the GDPR, 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,

(vii) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period,

(viii) 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,

(ix) where the processing is based on Article 6, paragraph (1), item a) or Article 9, paragraph (2), item a) of the GDPR, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal

(x) the right to lodge a complaint with the Hungarian National Authority for Data Protection and Freedom of Information,

(xi) the existence of automated decision-making, including profiling, referred to in Article 22, paragraph (1) and (4) of the GDPR 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.

4.1.2 Information to be provided where data are collected from the Data Subject

In case the Enterprise collects personal data from the Data Subject, further to the above, the Data Subject shall be informed whether providing personal data is based on legislation or contractual obligation, or if it is a prerequisite for concluding a contract, moreover, whether the Data Subject is obliged to provide personal data, and what the possible consequences of failure to data provision are.

Information shall be provided upon the acquisition of personal data. In case the Data Subject is already in possession of the above information, the notification thereof is unnecessary.

4.1.3 Information to be provided where data are not obtained from the Data Subject

In case the Enterprise collects personal data not from the Data Subject, further to the above, the Data Subject shall be informed about the personal categories thereof, the sources of personal data, and if applicable, whether the data originates from publicly accessible sources.

The Enterprise shall provide information at the following times:

(i) within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed,

(ii) if the personal data are to be used for communication with the Data Subject, at the latest at the time of the first communication to that Data Subject, or

(iii) if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

It is not necessary to provide the aforementioned data if

(i) the Data Subject already has the information,

(ii) 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, paragraph (1) of the GDPR, or in so far as the obligation referred to in paragraph 1 of this Article of the GDPR 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,

(iii) obtaining or disclosure is expressly laid down by EU or Member State law to which the controller is subject and which provides appropriate measures to protect the Data Subject's legitimate interests, or

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

4.2 Rights of the Data Subject

The Data Subject may request the Enterprise the access to and rectification or erasure of the relating personal data, the restriction of the processing thereof, and the exercise of the right to object. Furthermore, the Data Subject is entitled to the right to data portability and to legal remedy, and the right to decide on automated individual decision-making, including profiling.

Regarding certain rights of the Data Subject, The Enterprise shall provide information as part of the notification referred to in item 4.1.

4.2.1 The right of access

The Data Subject shall have the right to obtain from the Enterprise 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:

(i) the purposes of the processing in respect of a given personal data,

(ii) the categories of personal data concerned,

(iii) the categories of recipients to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations (in case of recipients in third countries or data transfer to international organisations, the Data Subject is entitled to request information regarding whether data transfer is subject to suitable safeguards),

(iv) the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period,

(v) rights of the Data Subject granted to the Data Subject (rectification, erasure, right to restrict, right to data portability, and the right to object to the control of such personal data),

(vi) the right to lodge a complaint with the Hungarian National Authority for Data Protection and Freedom of Information,

(vii) where the data are not collected by the Enterprise from the Data Subject, any available information as to their source,

(viii) the existence of automated decision-making, including profiling, regarding the personal data involved; if such decision-making has occurred, the information shall include the logic involved, as well as the significance and the envisaged consequences of such processing for the Data Subject.

Where the Data Subject makes the request by electronic form means, unless otherwise requested by the Data Subject, the information shall be provided in a commonly used electronic form.

Prior to responding to the request, the Data Subject may request the Enterprise to clarify the content thereof, and to clearly indicate the information requested and processing activities.

In case the Data Subject's right of access under the present item negatively impacts the rights and freedoms of other people (especially their trade secrets or intellectual property), the Enterprise is entitled to refuse the execution of the Data Subject's request to the necessary and proportionate extent.

In case the Data Subject requests the above notification in various copies, the Enterprise is entitled to charge a reasonable fee proportionate to the administrative expenses of producing surplus copies.

In case the data indicated by the Data Subject is not controlled by the Enterprise, the Data Subject shall be informed in writing thereof.

4.2.2 Right to rectification

The Data Subject is entitled to require the rectification of the personal data concerning him or her; in case the data are incomplete, the Data Subject may request the completion thereof.

When exercising the right to rectification/completion, the Data Subject shall indicate the data that are inaccurate or incomplete; furthermore, he or she shall provide the accurate and complete data. In duly substantiated cases, the Enterprise is entitled to ask the Data Subject to appropriately confirm the clarified data, in particular by an official document.

The rectification and completion of the data shall be performed by the Enterprise without unnecessary delay.

Following the fulfilment of the Data Subject's request to exercise his or her right to rectification, the Enterprise shall inform the recipients to whom the personal data of the Data Subject was communicated without delay, provided that it is not impossible or it does not involve disproportionate effort for the Enterprise. If required, the Data Subject shall be informed about these recipients.

4.2.3 Right to erasure ("right to be forgotten")

The Data Subject shall have the right to obtain from the Enterprise the erasure of personal data concerning him or her without undue delay, where one of the following grounds applies:

(i) the personal data indicated by the Data Subject are no longer necessary in relation to the purposes for which they were collected or otherwise processed by the Enterprise,

(ii) the personal data (involving sensitive data) was processed by the Enterprise based on the Data Subject's consent, who withdraws this consent in writing, and therefore, there is no other legal ground for the processing,

(iii) the Data Subject objects to the processing in relation to processing based on a legitimate interest of the Enterprise, and the Enterprise has no compelling legitimate reason overriding the Data Subject's interests, rights and freedoms, or connected to the establishment, exercise or defence of legal claims,

(iv) the personal data have been unlawfully processed by the Enterprise,

(v) the personal data processed by the Enterprise have to be erased for compliance with a legal obligation in EU or Member State law to which the Enterprise is subject,

(vi) the Data Subject objects to the data processing, and there are no overriding legitimate grounds for the processing.

The Data Subject shall submit his or her request in writing, indicating which personal data is to be erased for what reason.

In case of exercising the right of erasure, the Enterprise shall act in accordance with the rules of procedure described in item 4.3.

In case the Data Subject's motion for erasure is allowed by the Enterprise, the processed personal data shall be erased from each and every register, and the Data Subject shall be appropriately informed thereof.

In case the Enterprise is obliged to erase the personal data involved, the Enterprise shall take every reasonable step – including technical measures – necessary for communicating the obligatory erasure of personal data to controllers who received the personal data of the Data Subject as a result of the publication thereof. The Enterprise shall inform the other controllers that the erasure of links, copies or replications of the personal data of the Data Subject was requested by the Data Subject.

Following the fulfilment of the Data Subject's request to exercise his or her right to erasure, the Enterprise shall inform the recipients to whom the personal data of the Data Subject was communicated without delay, provided that it is not impossible or it does not involve disproportionate effort for the Enterprise. If required, the Data Subject shall be informed about these recipients.

The Enterprise is not obliged to erase personal data in case the data processing is necessary:

(i) for exercising the right of freedom of expression and information,

(ii) for the execution of the obligation to process personal data required from the Enterprise by Hungarian or EU legislation,

(iii) for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Enterprise,

(iv) for reasons of public interest in the area of public health,

(v) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, in so far as the Data Subject's right to be forgotten is likely to render impossible or seriously impair processing,

(vi) for the establishment, exercise or defence of legal claims.

4.2.4 Right to restriction of processing

The Data Subject shall have the right to obtain from the Enterprise the restriction of processing or use of personal data concerning him or her, where one of the following grounds applies:

(i) the accuracy of the personal data is contested by the Data Subject (in this case the restriction persists for a period enabling the Enterprise to verify the accuracy of the personal data),

(ii) the processing of personal data by the Enterprise is unlawful, but the Data Subject requests restriction instead of erasure,

(iii) the Enterprise 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,

(iv) the Data Subject objects to the processing in relation to processing based on a legitimate interest of the Enterprise, and the Enterprise has no compelling legitimate reason overriding the Data Subject's interests, rights and freedoms, or connected to the establishment, exercise or defence of legal claims; in this case the restriction persists until the verification of whether the legitimate grounds of the Enterprise override those of the Data Subject.

In case of restriction, 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 European Union or of a Member State.

A Data Subject shall be informed by the Enterprise before the restriction of processing is lifted.

Following the fulfilment of the Data Subject's request to exercise his or her right to restriction, the Enterprise shall inform the recipients to whom the personal data of the Data Subject was communicated without delay, provided that it is not impossible or it does not involve disproportionate effort for the Enterprise. If required, the Data Subject shall be informed about these recipients.

4.2.5 Right to object

In case the Enterprise does not perform data processing in the public interest or exercising its official authority, if it does not carry out scientific or historical research, and the processing does not have statistical purposes, the right to object may only be exercised in cases of processing based on legitimate interest.

In case the processing of the Data Subjects' personal data is based on legitimate interest, it is important to provide the Data Subjects with appropriate information regarding data processing and the right to object. Attention shall be drawn to the present right latest at the first communication to the Data Subject.

Based on the above, the Data Subject is entitled to object to processing his or her personal data, and if so, the Enterprise shall no longer process the personal data, unless it can be demonstrated that

(i) processing by the Enterprise is required by compelling legitimate grounds which override the interests, rights and freedoms of the Data Subject, or
(ii) processing is for the establishment, exercise or defence of the legal claims of the Enterprise.

4.2.5.1 Right to object to processing for direct marketing purposes

Regarding data processing for direct marketing (DM) purposes, the GDPR declares that in case of related data processing, the existence of legitimate interest may be supposed.

Therefore, in case of direct marketing activities carried out by the Enterprise, the Data Subject is also entitled to object to the processing of his or her personal data for such purposes; however, as opposed to data processing based on other legitimate interest, the Enterprise is not in a position to consider whether data can be further be processed in case of the Data Subject's objection.

In case the Data Subject objects to data processing for direct marketing purposes, the data of the Data Subject shall no longer be processed by the Enterprise for such purposes.

4.2.5.2 Profiling

Profiling consists of any form of automated processing of personal data regarding the Data Subject. Such evaluations may be used to analyse or predict aspects concerning the Data Subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements.

The right to object involves profiling based on legitimate interest, as a specific data processing operation. In case profiling is carried out for direct marketing purposes, as a result of the Data Subject's objection, profiling based on his or her personal data shall also be terminated without delay.

4.2.6 Right to data portability

The Data Subject shall have the right to receive the personal data concerning him or her and processed by the Enterprise in a structured, commonly used and machine-readable format, and have the right to transmit those data to another controller without hindrance from the Enterprise.

The right to data portability may be exercised in relation to the personal data provided by the Data Subject for the Enterprise, and

(i) data processing shall be based on the consent of the Data Subject or on a contract, and

(ii) data processing shall be carried out by automated means.

The Data Subject shall have the right, where technically feasible, to have the personal data transmitted directly from the Enterprise to the controller named in the request of the Data Subject.

Under the right to data portability, the data medium shall be provided to the Data Subject by the Enterprise free of charge.

In case the Enterprise's right to data portability adversely affects the rights or freedoms of others, in particular trade secrets or intellectual property, the Enterprise may refuse to act on the request of the Data Subject, to the extent necessary.

Carrying out actions under data portability does not mean the erasure (transfer, moving) of those data; they are documented by the Enterprise until the Enterprise has otherwise adequate purpose and/or legal grounds for data processing.

4.2.7 Right to automated individual decision-making, including profiling

The concept of "automated decision making" is not defined by the GDPR: practically, it includes all the mechanised procedures as a result of which the data entered is assessed exclusively by computer technology, without human interference, in accordance with predetermined aspects/algorithms, and the assessment results in a decision with significant consequences on the Data Subject (e.g. machine based decisions about the refusal of loan applications, or online personnel selection carried out without human intervention).

In essence, "profiling" (see definitions above) is about the automated assessment of the Data Subjects' personal features. In case automated decision-making, including profiling is carried out by the Enterprise regarding the personal data of the Data Subject, it shall be referred to in the data protection notification. In this case, the data processing notification shall contain information regarding the logic applied, and the significance and likely consequences of such processing on the Data Subject.

The Data Subject shall have the right to request not to be subject to exclusively automated decisions – including profiling – that would have legal effects on him or her, or would have similarly significant affects on him or her.

The Data Subject is not entitled to request exemption from decision-making based on automated processing, in case the decision is necessary for the conclusion or execution of a contract, if decision-making is made possible by EU or Member State law, or if the decision is based on the Data Subject's explicit consent.

In case automated processing is necessary for the conclusion or execution of a contract, or if it is based on the Data Subject's consent, the Data Subject shall have the right to request human intervention from the Enterprise, to express his or her point of view, and to challenge the decision.

The Enterprise shall make all efforts to avoid the involvement of sensitive categories of personal data in automated decision-making. In case it is inevitable, automated decision-making shall be carried out in respect of the sensitive categories of personal data only if data processing is based on the Data Subject's consent, or if it is necessary for public interest based EU or Member State legislation, furthermore, if adequate measures have been implemented in order to ensure the protection of the rights of the Data Subject.

4.2.8 Right to legal remedy

4.2.8.1 Right to lodge a complaint

In case the Data Subject considers that the processing of his or her personal data by the Enterprise infringes the provisions of the operative data protection legislation, especially those of the GDPR, the Data Subject shall obtain the right to lodge a complaint at the Hungarian National Authority for Data Protection and Freedom of Information (NAIH).

Website: http://naih.hu/
Address: 22/c. Szilágyi Erzsébet fasor, H-1125 Budapest
Postal address: H-1530 Budapest, PO Box: 5.
Telephone: +36-1-391-1400
Fax: +36-1-391-1410
E-mail: ugyfelszolgalat@naih.hu

The Data Subject shall obtain the right to lodge a complaint at the supervisory authority in another Member State, in particular that of the Data Subject's habitual residence, place of work, or the place of the alleged infringement.

4.2.8.2 Judicial review of the decision of the supervisory authority, and other judicial remedy

The Data Subject and the Enterprise shall have the right to effective judicial remedy against a legally binding decision of a supervisory authority concerning them, in particular regarding the exercise of investigative, corrective and authorisation powers by the supervisory authority or the dismissal or rejection of complaints. However, the right to an effective judicial remedy does not encompass measures taken by supervisory authorities that are not legally binding, such as opinions issued by, or advice provided by the supervisory authority.

Furthermore, the Data Subject shall have the right to an effective judicial remedy, where the supervisory authority competent pursuant to Articles 55 and 56 of the GDPR does not handle a complaint or does not inform the Data Subject within three months on the progress or outcome of the complaint lodged.

Proceedings against a supervisory authority should be brought before the courts of the Member State where the supervisory authority is established.

4.2.8.3 Right to access to justice (right of action)

The Data Subject, regardless of his or her right to lodge complaints, shall have the right to access to justice in case his or her rights under the GDPR were infringed during processing.

In accordance with Section 23 of Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information ("**Info Act**"), in the event of any infringement of the Data Subject's rights the

Data Subject has the right to contest the controller at court. The courts proceed as a matter of urgency. The suit may be filed by the Data Subject – at the choice thereof – also at the court of justice competent at the Data Subject's address or place of residence. For the contact details of Hungarian courts of justice please refer to http://birosag.hu/torvenyszekek.

Given that the Enterprise does not constitute a public authority of a Member State acting in the exercise of its public powers, the suit may be filed by the Data Subject also at the courts having authority and competency at the Member State where the Data Subject resides, in case the Data Subject's regular place of residence is in another Member State of the European Union.

4.2.8.4 Other options for the enforcement of claims

The Data Subject is entitled to entrust a non-profit-making organisation or association to act in the Data Subject's name for filing a complaint, seeking the judicial review of the decision of the supervisory authority, lodging an appeal, and/or enforcing the Data Subject's right to receive compensation. The entrusted non-profit-making organisation or association shall be one established in accordance with the legislation of an EU Member State, with the statutory objective of acting in the public interest, and guaranteeing the protection of the rights and freedoms of the Data Subject in relation to their personal data.

4.2.8.5 Right to compensation

The Enterprise shall reimburse any material or non-material damage suffered by any person as a result of an infringement of the following legislation:

(i) the GDPR,

(ii) delegated and implementing acts adopted in accordance with the GDPR,

(iii) Member State law specifying rules of the GDPR.

The Enterprise shall be exempt from damages liability if it proves that it is not in any way responsible for the event giving rise to the damage.

The damaged party may file his or her claims for compensation at the courts having authority and competency at the Member State described in item 4.2.8.3.

4.2.8.6 Administrative fines

Administrative fines are imposed by the Hungarian National Authority for Data Protection and Freedom of Information (NAIH) depending on the circumstances of each individual case, in addition to, or instead of measures referred to in points a) to h) and j) of Article 58, paragraph (2) of the GDPR. In accordance with Article 83 of the GDPR, the degree of the fine depends on various circumstances, e.g. the gravity of the infringement.

4.2.8.7 Criminal and/or administrative penalties

In accordance with Section 70 of the Info Act., in case during its proceedings the NAIH entertains the suspicion of a crime, it shall initiate a criminal procedure at the competent authorities, and in case of the suspicion of infringement or disciplinary offence, it shall initiate infringement or disciplinary proceedings at the competent authorities. The acting authority shall inform the NAIH about its position regarding the initiation of the procedure within 30 days, and regarding the results of the procedure within 30 days from the closure thereof.

4.3 Rules of procedure

The Enterprise shall act during the execution of the above information requirements and the implementation of its measures in accordance therewith. In addition to the special regulations set out above, the Enterprise shall act respecting the following regulations.

4.3.1 The assessment of requests

In relation to actions requested based on the rights of the Data Subject defined in items 4.2.1 – 4.2.7, the following rules of procedure shall be applied.

The request of the Data Subject shall be submitted to the staff member fulfilling the position of HR manager.

The request shall be submitted in writing as an electronic mail, or in paper format (in a form). In case the request is not submitted in a form by the Data Subject, the request shall be evaluated based on its content. In case the Data Subject's request is submitted electronically, information shall be provided electronically, if possible, unless otherwise requested by the Data Subject.

The Data Subject is obliged to indicate the personal data regarding which measures are requested from the Enterprise.

The request shall be assessed by the Enterprise within 1 (one) month of receipt of the request submitted in writing. If necessary, considering the complexity of the request and the number of requests being processed, the deadline for examining the request may be extended by 2 (two) months by the Enterprise. The Data Subject shall be informed about the extension and the reasons therefor within 1 (one) month of receipt of the request.

In case the request of the Data Subject is well-founded, the measures requested from the Enterprise shall be implemented within the procedural time limits, and a written notification regarding the implementation shall be provided for the Data Subject.

In case the Enterprise does not implement any measures in relation to the Data Subject's request, without delay, but latest within 1 (one) month of receipt of the request, the Data Subject shall be informed about the reasons for the delay, about the Data Subject's right to file a complaint at any supervisory authority, and to exercise his or her right to judicial remedy.

4.3.2 Fees for the information communicated, the notification provided, and the measures implemented

The information determined in items 4.1, 4.2.1 – 4.2.7 and 6.2, information regarding the rights of the Data Subject, and measures requested shall be provided by the Enterprise free of charge. Where requests from a Data Subject are manifestly unfounded or excessive, in particular because of their repetitive character, considering the administrative costs of the provision of information or notification requested, or the execution of a requested action, the Enterprise may either:

(i) charge a reasonable fee, or

(ii) refuse to act on the request.

4.3.3 Identification of the applicant

In case, the identity of the originator of the request complying with items 4.2.1 – 4.2.6 of the present policy is reasonably doubted by the Enterprise, it may request further information necessary for the identification of the Data Subject.

5 Data transfer

The personal data of the Data Subject may be transferred by the Enterprise for specified purposes, in particular for the execution of an already existing contract with a third person, and/or for the execution of obligations defined in legislation, resulting from the status of employer in an employment relationship.

In case of data transfer, except for data transfers based on legislation, the Enterprise shall only transfer the personal data of the Data Subject to recipients with a seat within the territory of the European Union, or to recipients providing sufficient guarantees for data processing to be complying with the requirements of the GDPR.

In case personal data are transferred by the Enterprise to a third country, i.e. a country outside the European Union, or to an international organisation (or data is made available for controllers in a third country, or for international organisations), the Enterprise shall make sure that the recipient in a third country or the international organisation ensures that the extent of safety of the personal data of the Data Subject is equal to that of the Enterprise, in accordance with Chapter V of the GDPR.

In case data transfer is carried out towards a third country or international organisation unable to provide the necessary protection of personal data in accordance with Chapter V of the GDPR (e.g. some Asian or African countries), data transfer shall only be carried out without the Data Subject's consent in case data transfer complies with those described in Article 49 of the GDPR; in lack thereof the Data Subject's explicit consent is necessary.

6 Personal data breach

In case of any personal data breach, the Enterprise shall comply with the following rules, and shall act in accordance therewith.

6.1 Notification of the supervisory authority

The Enterprise shall notify the supervisory authority about any personal data breach regarding the data processed by them, without undue delay after becoming aware thereof, and if possible, within 72 hours latest from becoming aware thereof, at least including the following:

(i) a description of the nature of the personal data breach, including categories and an approximate number of the Data Subjects involved, and the categories and approximate number of data involved in the breach,

(ii) the name and contact details of the data protection officer (if any) or other contact person providing further information,

(iii) the possible consequences originating from the personal data breach,

(iv) actions made or planned by the controller to remedy the personal data breach, including actions aiming at mitigating the possible negative consequences.

In case it is not possible to communicate the aforementioned data concurrently, they may be communicated to the supervisory authority later, in phases without undue further delay. Where such notification cannot be achieved within 72 hours, the reasons for the delay should accompany the notification.

It is not necessary to report the personal data breach in case it is unlikely to result in a risk to the rights and freedoms of natural persons. The likelihood and severity of the risk should be determined by

reference to the nature, scope, context and purposes of the processing, on the basis of an objective assessment. Risks could include for example Data Subjects experiencing discrimination, becoming victims of misused identity, suffering financial losses, having their good repute compromised, or suffering significant economic or social disadvantage as a result of the personal data breach.

6.2 Notification of the Data Subject

In case any Data Subject, especially an employee of the Enterprise, is informed about a personal data breach, he or she shall inform the representative or data protection officer of the Enterprise thereof, without delay. Fees regarding the notification shall be charged in accordance with item 4.3.2.

In each and every case where the personal data breach is likely to result in a high risk to the rights and freedoms of the Data Subject(s), and the Enterprise is informed about the breach, it shall inform the Data Subject(s) thereof without undue delay. The notification shall include, using clear and plain language, the following:

(i) the nature of the personal data breach,

(ii) the name and contact details of the data protection officer or other contact person providing further information,

(iii) the possible consequences originating from the personal data breach,

(iv) actions made or planned by the Enterprise to remedy the personal data breach, including, if applicable, actions aiming at mitigating the possible negative consequences originating from the personal data breach.

The notification of the Data Subject is unnecessary in case any of the following conditions is met:

(i) the Enterprise concluded the adequate technical and organisational protective actions, which were applied in relation to the data involved in the personal data breach, in particular actions that, e.g. by encryption, make the data incomprehensible for persons not authorised to access those personal data,

(ii) subsequent to the personal data breach, the Enterprise carried out further actions ensuring that the high risk to the rights and freedoms of the Data Subject are unlikely to occur,

(iii) the notification would involve disproportionate effort. In such a case, there shall instead be a public communication, through information published in a locally usual manner, or similar measure whereby the Data Subjects are informed in an equally effective manner.

If the Enterprise 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 communication to the Data Subject by the Enterprise, or may decide that any of the aforementioned conditions are met, therefore the notification of the Data Subject to be unnecessary.

7 Records of processing

7.1 Records of processing activities

The Enterprise and the Enterprise's representative shall maintain a record of processing activities under its responsibility in writing, including electronic documents, in accordance with Article 30 of the GDPR. That record shall contain all of the following information:

(i) the name and contact details of the Enterprise and, where applicable, the joint controller, the controller's representative and the data protection officer,

(ii) the purposes of the processing,

(iii) a description of the categories of Data Subjects and of the categories of personal data,

(iv) the categories of recipients to whom the personal data have been or will be disclosed, including recipients in third countries or international organisations,

(v) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49, paragraph (1) of the GDPR, the documentation of suitable safeguards,

(vi) where possible, the envisaged time limits for erasure of the different categories of data,

(vii) where possible, a general description of the technical and organisational security measures referred to in Article 32, paragraph (1) of the GDPR.

The Enterprise and the Enterprise's representative shall make the record available for the supervisory authority on request.

7.2 Documentation of personal data breaches

The Enterprise shall document any personal data breaches, comprising the following:

(i) facts relating to the personal data breach,

(ii) its effects and

(iii) the remedial action taken.

The Hungarian National Authority for Data Protection and Freedom of Information shall have the right to access the present documentation to verify compliance with Article 33 of the GDPR.

8 Data protection officer (DPO)

The Enterprise doesn't have a DPO.

9 Data protection impact assessment

Data protection impact assessment is about the obligation of the Enterprise to carry out impact assessment in case of data processing which is likely to imply high risk on the rights and freedoms of natural persons (see in particular Article 35, paragraph (3) of the GDPR). The impact assessment shall contain at least the following information:

(i) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller,

(ii) an assessment of the necessity and proportionality of the processing operations in relation to the purposes,

(iii) an assessment of the risks to the rights and freedoms of the Data Subject,

(iv) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR taking into account the rights and legitimate interests of data subjects and other persons concerned.

10 Training

The Enterprise or its data protection officer shall ensure raising awareness of data protection for those participating in data processing at the Enterprise, and the training thereof (organisation, regularity, examination, legal consequences, revision, etc.).

11 Processing

The Enterprise uses processors for the completion of technical tasks related to data processing procedures. The rights and obligations of the processors in connection with processing personal data are defined by the GDPR, and the Enterprise – as controller – within the rules of law on data processing. The Enterprise is responsible for the lawfulness of its instructions given to the processor. The processor cannot make a substantive decision on the processing, the processor can only process the personal data pursuant to the instructions of the Enterprise, the processor cannot process the personal data for its own purposes, and the processor has to store and maintain the personal data pursuant to the instructions of the Enterprise.

12 Security of processing

"clean desk policy", password-protected user accounts, terminals and laptops,

Other provisions

In the present Policy European Union legislation and European Union shall include legislation to be applied in the member states of the European Economic Area and the member states of the EEA.

13 Effect and review order

The Policy came into effect on 25 May 2018, and stays valid until revocation. With the Policy's entry into force, each and every previously applicable policy in the subject of the present Policy becomes ineffective.

At least once in every year, including the date of entry into force of the Policy, it shall be revised, and the revision shall fully cover the contents of each and every annex.

Every representative, officer, and agent of the Enterprise shall be obliged to observe and respect the applicable regulations of the Policy, and they shall carry out their functions in full compliance with the specifications of the Data Processing Policy.

In case of legislative amendment, furthermore, in the event of modifying the present Policy for other reasons, the Enterprise publishes the amended version of the present Policy on its website.

Budapest, 25 May 2018

Aliz Tech Kft.

Acting on behalf thereof: István Boscha Executive Director