PRIVACY POLICY

Name of the Controller:	UNI-INVEST Kft. (hereinafter: Company or Enterprise)
Controller's corporate registration number:	01-09-079613
Controller's registered seat:	1094 Budapest, Tűzoltó utca 57.
Controller's e-mail address:	kopont@uni-invest.hu
Controller's representative:	Mr. Ferenc Karacs, managing director

Interpretation

data processor: means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller

data processing: means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, 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 Enterprise, the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of personal data processing; 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

data protection incident: a violation of security that results in incidental or unlawful annihilation, loss, change, authorized publication of, and unauthorized access to transferred, stored data or data processed in another manner

biometric data: means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data

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

health data: means 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 whose personal data are processed

consent by the data subject: any freely given, specific, informed and unambiguous indication of the data subject's wishes by which s/he, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him/her

supervisory authority: means an independent public authority which is established by an EU Member State pursuant to Article 51 of the GDPR

GDPR: Regulation (EU) 2016/679 of the European Parliament and of the Council 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)

genetic data: means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question

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

sensitive data: personal data pertaining to the special category of personal data, 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: means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to 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 personal data categories: 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

1. Purpose of the Policy

The purpose of this Privacy Policy is to introduce and consistently apply measures that guarantee the accurate and safe processing of the Data Subjects' personal data in compliance with the effective data protection laws of the EU and its Member States, implemented uniformly at the level of the Enterprise. At the same time, the Privacy Policy provides concise, transparent and easily accessible information to the Data Subjects about access to their personal data processed by the Enterprise, furthermore it provides the rules under which the Enterprise safeguards the rights of the Data Subjects.

2. Basic data processing principles

Prior to starting the processing of personal data it must be carefully considered in each case whether it is actually necessary.
The processing of personal data may only be started if it can be justified without any doubt that the purpose of data processing cannot be achieved in any other manner.

The Enterprise shall process the Data Subjects' personal data lawfully, in a fair and transparent manner. No one shall suffer any disadvantage due to initiating or reporting a procedure or legal remedy at the Enterprise or at any other authority specified herein and due to refusing or withdrawing their consent in the case of consent-based data processing.

The personal data of Data Subjects may only be collected for a defined, clear and lawful purpose. The Enterprise is obliged ab ovo to avoid – and to terminate later – any data processing that is done in a manner not compatible with the purpose relevant to the given personal data. The Enterprise is entitled to process personal data only to the required extent and it shall erase all personal data where the purpose of data processing ceased to exist, or the legal ground of data processing cannot be verified.

The Company shall introduce control mechanisms that are suitable for ensuring both in advance and subsequently – by screening - that

(i) the personal data fulfill the purposes of data processing already at the date of data collection, and then during the full period of data processing, furthermore
(ii) the amount of data processing is limited to the necessary level in terms of both the circle of data and the period of data processing.

The personal data processed by the Enterprise shall be accurate and up-to-date. The Company shall take all reasonable measures to ensure that accurate personal data are processed,
(i) personal data that are superfluous, or become superfluous in the meantime from the viewpoint of data processing are erased without delay;
(ii) inaccurate personal data are rectified or erased.

Personal data shall be stored in a manner that it enables the identification of Data Subjects only for the period required for achieving the purposes of data processing.

Personal data shall be processed in a manner that ensures - by using appropriate technical or organisational measures - appropriate security of the personal data, including all actions that provide protection against unauthorised or unlawful processing and against accidental loss, destruction or damage of personal data.

3. Lawfulness of data processing

The pre-condition of lawful data processing is that the ground for data processing should be properly defined and further conditions pertaining to the selected legal ground should be fulfilled. Therefore, the requirement of lawfulness – in a narrower sense - presumes that an appropriate legal ground for data processing exists, and in a narrower sense it means that personal data may only be processed in harmony with the laws governing the given legal ground for data processing.

With a view to the activities pursued by the Company, the following main legal grounds can be selected for the personal data of the Data Subjects, subject to the type and the circumstances of data processing.

The main legal grounds mentioned in the first sub-paragraph refer to all personal data, except for the special categories of personal data, while the second sub-paragraph lays down special provisions related to the legal grounds for special categories of personal data.

3.1. Personal data, not including special personal data categories

The Company may process the personal data of the Data Subjects – excluding sensitive data – especially under the following legal grounds:

- Consent: Data Subjects may give consent to processing their personal data if it can be proved that their consent is voluntary. If the Enterprise processes the personal data of children aged under 16 with regard to information society related services offered to children aged under 16, as a main rule, data processing is lawful only if, and to the extent where the consent was given or permitted by the person exercising parental supervision over the child. Data subjects give their consent on a voluntary basis and they may withdraw it at any time. The withdrawal shall not affect the lawfulness of previously implemented data processing.
- Preparing and fulfilling contracts: This legal ground can be applied for data processing needed for contractual fulfilment (e.g. contract for providing services, employment contract, study contract), where the Data Subject is one of the parties, or data processing is needed for taking actions upon request by the Data Subject prior to signing the contract.
- Fulfilling legal obligations: Data processing required by an EU or national law.
- Legitimate interest: This includes data processing required for enforcing the legitimate interests of the Enterprise or a third party. The legitimate interest of the Enterprise or a

third party is stipulated in the privacy notice relevant for the given data processing purpose. Data may be processed based on a legitimate interest only in the case where the Enterprise makes an interest assessment test to check and record if the Enterprise's legitimate interest limits the Data Subjects' privacy and the right to the protection of personal data in a proportionate manner and how the balance can be set up between the interests of the Enterprise and the Data Subjects. The interest assessment test is not a part of the privacy notice.

If the Enterprise collects data from the Data Subjects and the Data Subjects do not disclose the data processed on the above legal grounds, a possible consequence of data supply can be the refusal or the impossibility of preparing or fulfilling a contract (e.g. failure to establish employment). If the Data Subjects fail to supply only a part of the data that are to be supplied, it must be judged based on the partially supplied data whether the failure of data supply can cause e.g. the impossibility to conclude or maintain the contract. In the case of contract-based data processing, the Enterprise may apply the legal consequences of impossibility only if it is verified that the Data Subject is unable to fulfill the contract without the supplied data.

3.2. Sensitive data

Sensitive data imply risks and require special protection due to their nature and with a view to the basic rights and freedoms that natural persons are entitled to. The Enterprise may process the sensitive data of Data Subjects – primarily including health data – especially for the following purposes and under the following legal grounds:

- Article 9 (2) a) of the GDPR: Data Subjects may give consent to processing their personal data if it can be proved that the consent is voluntary. The Data Subjects give their consent voluntarily and may withdraw it at any time. The withdrawal shall not affect the lawfulness of previously implemented data processing.
- Article 9 (2) b) of the GDPR: The Enterprise may process data for the purposes of carrying out the obligations and exercising specific rights in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law.
- Article 9 (2) f) of the GDPR: This legal ground can be applied if processing sensitive data is necessary for submitting, enforcing or defending legal claims.

4. Obligation of the Company to provide information and take actions

The Enterprise shall notify the Data Subjects and provide them with specific information about their rights in a concise, clear, transparent, easy-to-access and easy-to-understand form. Furthermore, the Enterprise may take measures upon request by the Data Subjects, by observing certain procedural rules.

4.1. Privacy Notice

The Enterprise shall supply the Data Subjects with certain information on data processing depending on whether the personal data are collected from the Data Subjects or not. The common and individual rules of this data processing information are summarized by the following sub-chapters.

4.1.1. Common rules

Based on the obligation to provide information, the Enterprise shall notify the Data Subjects in the following cases:

- the identity and the contact details of the Enterprise and, where applicable, of the Enterprise's representative,
- the purpose of processing the personal data and the legal basis for data processing,
- where the processing is based on point (f) of Article 6(1) of the GDPR, the legitimate interests of the Enterprise or a third party,
- where applicable, the recipients or categories of recipients of the personal data, if any,
- where applicable, the fact that the Enterprise intends to transfer the personal data to a third country or to an international organization, furthermore the existence or absence of an adequacy decision by the European Commission, or in the case of data transfers referred to in Article 46 of the GDPR, 47 of the GDPR or the second sub-paragraph of Article 49 (1) of the GDPR, reference to the appropriate or suitable safeguards, to the means of obtaining a copy of them or to their accessibility,
- the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period,
- the existence of the Data Subject's right to request from the controller access to and rectification or erasure of personal data or restriction of processing or to object to processing as well as the right to data portability,
- where the processing is based on point (a) of Article 6 (1) of the GDPR or point (a) of Article 9 (2) of the GDPR, the existence of the right to withdraw consent at any time, without affecting the lawfulness of consent-based processing before its withdrawal,
- the right to lodge a complaint with a supervisory authority,
- the existence of automated decision-making, including profiling, referred to in Article 22 (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 Subjects

If the personal data are collected by the Enterprise from the Data Subjects, apart from the above, it shall notify the Data Subjects whether the supply of personal data is a statutory or contractual requirement or a pre-condition on concluding a contract, as well as whether the data subject is

obliged to provide the personal data and what are the possible consequences of failing to provide such data.

The information shall be given at the date of acquiring the personal data. However, if the Data Subjects already have the above information, it is not necessary to notify them.

4.1.3. Information to be provided where data are not collected from the Data Subjects

If the Enterprise collects the personal data not from the Data Subjects, it shall notify the Data Subjects – apart from the above information – about the Data Subjects' personal categories and about the source of the personal data and, in the given case, whether the data derive from publicly available sources.

The Enterprise shall provide the information at the following dates:

- 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,
- if the personal data are to be used for communication with the Data Subjects, at least at the time of the first communication with the Data Subjects, or
- 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 above data if

- the Data Subject already has the information,
- the provision of such information proves impossible or would involve disproportionately large efforts, 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) of the GDPR 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,
- obtaining or disclosing the data is expressly laid down by the 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
- 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.

4.2. Rights of the Data Subjects

The Data Subjects may request from the Enterprise access to, and rectification or erasure of personal data or the limitation of processing and they may object to processing such personal data.

Furthermore, the Data Subjects have the right to data portability and legal remedy as well as the right to decide on automated decision-making applied in individual cases, also including profiling.

The Enterprise shall give information about certain rights of the Data Subjects as a part of the information set forth in paragraph 4.1.

4.2.1. Right to access

Data Subjects have the right to obtain from the Enterprise confirmation as to whether or not their personal data are being processed, and, where that is the case, they are entitled to access the personal data and the following information:

- Purposes of data processing with regard to the given personal data,
- Categories of the personal data concerned,
- Categories of recipients to whom the personal data of the Data Subject have been, or will be communicated, especially including recipients in third countries and international organizations (if data are forwarded to recipients in third countries and international organizations, the Data Subject may request information as to whether the data are forwarded under appropriate safeguards),
- The period for which the personal data concerned are planned to be stored, or if that is not possible, the criteria used to determine that period,
- Rights of the Data Subject (right to rectification, erasure or limitation, right to data portability, as well as the right to object to processing such personal data),
- Right to lodge a complaint with a supervisory authority,
- Where the data are not collected by the Enterprise from the Data Subject, any available information as to their source,
- The fact of automated decision-making regarding the personal data concerned, also including profiling; if data are processed in this manner, the information shall cover the applied logic as well as the expected significance and the envisaged consequences of such processing for the Data Subject.

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

Before fulfilling the request, the Enterprise may request the Data Subject to correct the contents of the request and to accurately indicate the requested information and data processing activities.

If the access right of the Data Subject hereunder adversely affects other people's rights and freedoms, thus specifically other people's business secrets or intellectual property, the Enterprise may reject the fulfilment of the Data Subject's request at the required and proportionate rate.

If the Data Subject requests several copies of the above information, the Enterprise may charge an administrative fee that is reasonable and proportionate with making extra copies.

If the Enterprise does not process the personal data indicated by the Data Subject, the Enterprise shall also notify the Data Subject about this fact in writing.

4.2.2. Right to correction

Data Subjects have the right to request correction of their personal data. If the personal data relevant to the Data Subject are deficient, the Data Subject may request supplementation of the personal data.

When exercising the right to correction/supplementation, the Data Subject shall indicate which data are inaccurate or deficient and shall also inform the Enterprise about the full and accurate data. In a justified case, the Enterprise may call on the Data Subject to evidence the corrected data to the Enterprise in an appropriate manner, primarily through documents.

The Enterprise shall correct and supplement the data without unjustified delay.

After fulfilling the Data Subjects' request to enforce their right to correction, the Enterprise shall immediately notify the persons to whom the Data Subjects' personal data were disclosed, provided that, it is not impossible, or it does not require disproportionate efforts from the Enterprise. The Enterprise shall inform the Data Subject about those recipients if requested by the Data Subject.

4.2.3. Right to erasure ('right to be forgotten')

The Data Subjects may request the Enterprise to delete their personal data without any unjustified delay if any of the below reasons prevail:

- The personal data indicated by the Data Subject are no longer necessary in relation to the purpose for which they were collected or otherwise processed by the Enterprise,
- The Enterprise processed the personal data (also including sensitive data) based on the Data Subjects' consent, the Data Subjects withdrew their consent in writing and the data processing has no other legal ground,
- The Data Subject objects to data processing that is based on the Enterprise's legitimate interest, and the Enterprise has no compelling legitimate grounds for the processing which override the interests, rights and freedoms of the Data Subject or which are connected to the submittal, enforcement or defense of legal claims,
- The Enterprise processed the personal data unlawfully,
- The personal data processed by the Enterprise have to be erased for compliance with a legal obligation set forth in an EU or Member State law to which the Enterprise is subject,
- The Data Subjects object to data processing and there is no overriding legal ground for data processing.

The Data Subjects shall submit their erasure request in writing and shall indicate what personal data should be erased and for what reason.

When exercising the right to erasure, the Enterprise shall act in consideration of the procedural rules specified in paragraph 4.3.

If the Enterprise accepts the Data Subjects' erasure request, it shall erase the processed personal data from all records and shall appropriately notify the Data Subjects about this fact.

If the Enterprise is obliged to delete the Data Subjects' personal data, the Enterprise shall take all reasonable measures – also including technical measures – that are also required for notifying those controllers about the obligatory erasure of the personal data who accessed the Data Subjects' personal data as a result of their disclosure.

In the notification the Enterprise shall notify the other controllers about the fact that the Data Subjects requested erasure of the links to their personal data or erasure of the copy or copies of such personal data.

After fulfilling the Data Subjects' request to enforce their right to erasure, the Enterprise shall immediately notify the persons to whom the Data Subjects disclosed their personal data, provided that, it is not impossible, or it does not require disproportionate efforts from the Enterprise. The Enterprise shall inform the Data Subject about those recipients if requested by the Data Subject.

The Enterprise is not obliged to erase personal data if data processing is required for:

- Exercising the right of freedom to express opinion and to receive information,
- Fulfilling the obligation of personal data processing imposed on the Enterprise by a Hungarian or EU law,
- Performing a task carried out in the public interest or within the framework of exercising public authority vested in the Enterprise,
- Implementing a public interest concerning the area of public health,
- Archiving in public interest and for scientific and historical or statistical purpose, provided that data processing would probably become impossible or seriously endangered if the Data Subject exercised his/her right to be forgotten,
- Establishing, enforcing or defending legal claims.

4.2.4. Right to limit data processing

Data Subjects may request the Enterprise to limit processing and the use of their personal data without delay if any of the below reasons prevail:

- The accuracy of the personal data is contested by the Data Subject (in this case, the limitation lasts until the Enterprise verifies the accuracy of the personal data),
- The Enterprise processed the personal data unlawfully but the Data Subject requests limitation instead of erasure,
- The purpose of data processing ceased to exist for the Enterprise, but the Data Subject requires them in order to submit, enforce or protect legal claims,

- The Data Subject objects to data processing that is based on the Enterprise's legitimate interest, and the Enterprise has no compelling legitimate grounds for processing which override the interests, rights and freedoms of the Data Subject or that are connected to the submittal, enforcement or defense of legal claims; in this case, the limitation exists until it is established whether the Enterprise's legitimate reasons are given priority over the Data Subject's legitimate reasons.

In the case of limitation, personal data shall, with the exception of storage, only be processed with the Data Subject's consent or for the submittal, enforcement or defence of legal claims or for the protection of the rights of another natural person or legal entity or in the important public interest of the European Union or a Member State.

The Enterprise shall be previously inform the Data Subject about terminating the limitation of data processing.

After fulfilling the Data Subjects' request to enforce their right to limitation, the Enterprise shall immediately notify the persons to whom the Data Subjects disclosed their personal data, provided that, it is not impossible, or it does not require disproportionate efforts from the Enterprise. The Enterprise shall inform the Data Subject about those recipients if requested by the Data Subject.

4.2.5. Right to object

Exercising the right to object may arise in the case of data processing based on a legitimate interest since the Enterprise deals with no data processing in public interest and has no public authority either, conducts no scientific or historical research and no data are processed for statistical purposes.

If the data of the Data Subjects are processed based on a legitimate interest, it is an important, safeguard-type provision that proper information and the enforcement of the right to object must be guaranteed for the Data Subjects with regard to data processing. The attention of the Data Subject shall be expressly drawn to this right at the latest upon making the first contact.

Based on this, the Data Subjects may object to processing their personal data, and in this case the Enterprise may no longer process the Data Subjects' personal data unless it can be proved that

- Data processing by the Enterprise is justified by compelling legitimate reasons that are given priority over the Data Subjects' interests, rights and freedoms, or
- Data processing is required for submitting, enforcing or protecting the legal claims of the Enterprise.

4.2.5.1. Right to object in the case of direct marketing

In the event of data processing for direct marketing, the GDPR also recognizes that the existence of the legitimate interest can be presumed in the case of related data processing.

Therefore, in the case of direct marketing activities pursued by the Enterprise, the Data Subjects may also object to processing their personal data for this purpose, however, as against data processing based on other legitimate interest, the Enterprise may not consider – as a result of the objection – whether the data processing can still be continued if objected by the Data Subject.

If the Data Subject objects to data processing for the purpose of direct marketing, the personal data of the Data Subject may no longer be processed by the Enterprise for this purpose.

4.2.5.2. Profiling

Upon profiling the personal features of the Data Subjects are assessed through various automated methods. Such assessments may be used, e.g. for analyzing or forecasting the Data Subjects' characteristics related to work performance, economic status, health condition, personal preferences, interests, reliability, behaviour, place of residence or movement.

The right to object also covers profiling based on a legitimate interest, as a specific data processing operation. If profiling is carried out for the purpose of direct marketing, personal data-based profiling shall also be terminated if it is objected by the Data Subject.

4.2.6. Right to data portability

Data Subjects have the right to receive their personal data processed by the Enterprise in a structured, commonly used and machine-readable format and have the right to transfer those data to another controller without any limitation by the Enterprise.

The right to data portability may be exercised for personal data that the Data Subject disclosed to the Enterprise and

- Data processing is based on the Data Subject's consent or on a contractual legal ground and
- Data processing is carried out by automated means.

If technically feasible, the Enterprise transfers the personal data, upon request by the Data Subject, directly to another controller specified in the Data Subject's request. The right to data portability hereunder shall not raise any obligation for the controllers to introduce or maintain technically compatible data processing systems with each other.

Within the scope of data portability, the Enterprise shall provide the data carrier to the Data Subject free of charge. If the right of the Data Subject to data portability affects adversely other people's rights and freedoms, thus specifically other people's business secrets or intellectual property, the Enterprise may reject the fulfilment of the Data Subject's request to the required extent.

Action taken with regard to data portability shall not mean deletion of the data, but the Enterprise continues to record them until it has an appropriate purpose and legal ground for data processing.

4.2.7. Right to decide on automated decision-making in individual cases, including profiling

The GDPR does not define the term of automated decision-making, but basically it covers all processes whereby the entered data are assessed exclusively with computerized tools, without human intervention, under pre-defined aspects/algorithm, and the decision made as a result of this assessment involves significant consequences for the Data Subject.

The GDPR mentions as an example the rejection of online credit applications through automatic decision-making, or online labour force selection without human intervention.

As against this, the term of profiling is accurately specified and laid down in the GDPR, as can also be seen in the previous paragraph, and the point is that the personal characteristics of the Data Subjects are assessed with some automated method. If the Enterprise makes an automated decision on the Data Subject's personal data, also including profiling, it shall be mentioned in the Privacy Notice. In this case, the Privacy Notice contains information about the applied logic, as well as the significance and the envisaged consequences of such data processing for the Data Subject.

Data Subjects have the right to request not to be affected by the scope of the decision exclusively based on automated data processing, also including profiling, which would impose a legal impact on them or would affect them in a similarly significant manner. Data Subjects may not request exemption from the effect of the decision based on automated data processing if the decision is required for concluding or fulfilling a contract or the decision-making is facilitated by an EU or Member State law or the decision is based on the Data Subject's express consent.
If automated data processing is required for concluding or fulfilling a contract or it is based on the Data Subjects' consent, the Data Subjects have the right to request human intervention from the Enterprise, to express their standpoint and to submit a complaint about the decision.

In the course of data processing, the Enterprise shall do its best not to involve in automated decision-making data pertaining to special personal data categories. If, however, this cannot be avoided, automated decision can be made about the special categories of personal data only if data processing is based on the Data Subjects' consent or it is required for a significant public interest based on the law of the EU or a Member State and appropriate measures have been taken in order to protect the Data Subjects' rights.

4.2.8. Right to legal remedy

4.2.8.1. Right to complaint

If the Data Subjects find that processing their personal data by the Enterprise violates the provisions of the effective privacy regulations, thus specifically those of the GDPR, they may submit a complaint to the Hungarian National Authority for Data Protection and Freedom of Information (Nemzeti Adatvédelmi és Információszabadság Hatóság).

Contacts of the Hungarian National Authority for Data Protection and Freedom of Information:
Website: http://naih.hu/
Address: 1125 Budapest, Szilágyi Erzsébet fasor 22/c.
Mail address: 1530 Budapest, Pf.: 5.
Telephone: +36-1-391-1400
Fax: +36-1-391-1410
E-mail: ugyfelszolgalat@naih.hu

Data subjects may also submit a complaint to another supervisory authority, especially established in the EU Member State of their usual residence, workplace or at the place of the presumed violation of law.

4.2.8.2. Judicial supervision of the resolution by the supervisory authority and other legal remedies

The Data Subjects and the Enterprise are entitled to effective judicial remedy against the relevant binding resolution of the supervisory authority, thus specifically against the resolution of the supervisory authority on exercising the investigation, correction and licensing powers of the supervisory authority as well as on rejecting complaints or regarding them as unfounded.

However, the right to an effective judicial remedy does not encompass measures taken by supervisory authorities which are not legally binding, such as opinions issued, or advice provided by the supervisory authority.

Furthermore, each Data Subject shall have the right to effective judicial remedy if the supervisory authority which is competent pursuant to Articles 55 and 56 of the GDPR does not handle the complaint or does not inform the Data Subject within three months on the progress or outcome of the lodged complaint. Proceedings against a supervisory authority shall be brought before the courts of the EU Member State where the supervisory authority is established.

4.2.8.3. Right to turn to court (right to start an action)

Data Subjects may turn to court – regardless of their right to submit a complaint – if their rights specified in the GDPR have been violated upon processing their personal data. A lawsuit may be started at a Hungarian court against the Enterprise, being a controller pursuing its activities in Hungary.

Data Subjects may also institute the lawsuit at the court competent at their residence, under article 22 (1) of the current Info Act. The availability of Hungarian courts can be found through the following link: http://birosag.hu/torvenyszekek.

Since the Enterprise is not regarded as a public authority organization acting by exercising the public authority licenses of a Member State, the Data Subject may also launch the lawsuit at a court having power and competence at the place of usual residence if the place of usual residence of the Data Subject is in another Member State of the European Union.

4.2.8.4. Other options for enforcing claims

Data Subjects have the right to mandate a non-profit body or association - which has been properly constituted in accordance with the law of an EU Member State, has statutory objectives which are in the public interest and is active in the field of protecting the Data Subjects' rights and freedoms with regard to their personal data - to lodge the complaint on their behalf, to carry out a court review of the resolution of the supervisory authority, to file an action or to exercise the right to receive compensation on behalf of the Data Subjects.

4.2.8.5. Right to damages

The Enterprise shall reimburse the financial or non-financial damage suffered by another person as a result of violating the following regulations:

- GDPR,
- Authorization-based legal acts adopted in compliance with the GDPR as well as legal acts for implementation,
- Member state laws refining the GDPR regulation.

The Enterprise shall be exempt from the liability for damages if it proves that it is in no way responsible for the event giving rise to the damage.
The injured party may submit his/her claim for damages to the court having power and competence in the Member State specified in paragraph 4.2.8.3.

4.3. Procedural rules

When providing the above obligatory information and taking action, the Enterprise shall proceed as specified above. In addition to the above specified rules, the Enterprise shall proceed in keeping with the following regulations.

4.3.1. Judging the request

The following procedural rules shall apply for the actions requested with regard to the Data Subjects' rights set forth in paragraphs 4.2.1 – 4.2.7.

The Data Subjects may submit their requests to the HR associate.

The request may be submitted in writing, via e-mail or on paper. If the Data Subject does not submit the request in a form sheet, the request shall be judged based on its contents. Where the Data Subject makes the request in an electronic form, the information shall possibly be provided in an electronic form, unless otherwise requested by the Data Subject.

In their request the Data Subjects shall indicate the personal data for which they request action by the Enterprise.

The Enterprise shall judge the request within 1 (one) month from receipt of the request submitted in writing. The Enterprise may extend the deadline for judging the request by another 2 (two) months where necessary, taking into account the complexity and number of the requests in progress. The Enterprise shall inform the Data Subject of any extension, together with the reasons for the delay, within 1 (one) month from receipt of the request.

If the request of the Data Subject is well-founded, the Enterprise shall take the requested action within the procedural deadline and notifies the Data Subject about the implementation in writing.

If the Enterprise does not take action in response to the request of the Data Subject, the Enterprise shall inform the Data Subject without delay but at the latest within 1 (one) month from receiving the request about the reasons for not taking action and about the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

4.3.2. Fee for the information provided and action taken

The Enterprise provides the information under 4.1, 4.2.1 – 4.2.7 and 6.2, the information about the Data Subjects' rights and takes the requested actions free of charge. However, where the request from a Data Subject is manifestly unfounded or excessive, in particular because of its repetitive character, the Enterprise may - with regard to the administrative costs of providing the requested information or taking the requested action -

- May charge a reasonable fee or
- May refuse to act based on the request.

4.3.3. Checking the personal identity of the requesting party

If the Enterprise has any well-founded doubts about the identity of the person submitting the request under paragraphs 4.2.1 – 4.2.6 hereof, the Enterprise may request the Data Subject to provide further information to confirm his/her personal identity.

5. Data transfer

The Enterprise may transfer the Data Subjects' personal data for specific purposes, thus specifically in order to fulfill contracts concluded with a third party or to fulfill obligations set forth in the laws or employer obligations arising from employment.

In the case of data transfer, except for data transfer based on the laws, the Enterprise may transfer the Data Subjects' personal data exclusively to recipients that have a registered seat in the area of the EU or provide appropriate safeguards that their data processing complies with the provisions of the GDPR.

If the Enterprise transfers personal data to a third country – i.e. outside the EU – or to an international organization (or makes them accessible to a Company or international organization operating in a third country), the Enterprise shall ensure that the recipient or international

organization operating in the third country provides the same protection of the Data Subjects' personal data as the protection provided by the Enterprise, as set forth in chapter V of the GDPR.

If data are transferred to a third country or international organization that cannot provide the appropriate level of protection of personal data as set forth in chapter V of the GDPR (e.g. certain Asian or African countries), data may only be transferred without the consent of the Data Subjects only if the data transfer complies with the provisions of Article 49 of the GDPR; in the lack of this, the Data Subjects' express consent is required for transferring personal data.

6. Data protection incident

In the case of data protection incidents the Enterprise shall observe the following rules and shall act based on the following rules.

6.1. Report to the supervisory authority

With regard to the processed data, the Enterprise shall report any data protection incident to the supervisory authority without undue delay after learning about such a data protection incident, if possible at the latest within 72 hours after learning about the data protection incident, at least with the following contents:

- describing the nature of the data protection incident, including the categories and the approximate number of the Data Subjects concerned and the categories and the approximate number of the personal data affected by the incident,
- name and contacts of the data protection officer or any other contact person where more information can be obtained,
- likely consequences of the data protection incident,
- actions taken or planned by the Company to address the data protection incident, including, where appropriate, actions to mitigate its possible adverse effects.

Where, and in so far as, it is not possible to provide the above information at the same time, the information may be provided to the supervisory authority in phases, without undue further delay. Should the report not be made within 72 hours, the reasons verifying the delay shall also be attached to it.

It is not necessary to report the data protection incident if the data protection incident probably involves no risk for 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, based on objective assessment. For example, it may be qualified as a risk if the Data Subjects are discriminated due to the incident, may become subjects of abuse with their personal identity, may suffer financial loss, their good reputation may be damaged, or they may suffer other significant economic or social disadvantage.

6.2. Informing the Data Subjects

If Data Subjects – especially the employees of the Enterprise - are notified about any data protection incident, they shall immediately inform the representative of the Enterprise. The provisions of paragraph 4.3.2 shall appropriately apply for fee calculation regarding the notification.

In all cases where the data protection incident probably involves a high risk for the rights and freedoms of any Data Subject/s and the Enterprise learns about the incident, it shall notify the Data Subject/s about it without unreasonable delay. The information shall disclose in a clear and easy-to-understand manner:

- The nature of the data protection incident,
- The name and availability of the contact person,
- The likely consequences of the data protection incident,
- The measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

The Data Subject does not have to be informed if any of the following conditions take place:

- The Enterprise took appropriate technical and organizational actions and these actions were applied for data affected by the data protection incident, especially actions – e.g. applying encryption – that make the data uninterpretable by persons not authorized to access the personal data,
- After the data protection incident the Enterprise took further actions to guarantee that the high risk affecting the Data Subject's rights and freedoms will presumably not take place in the future,
- The information would require disproportionate efforts, In such cases, the Data Subjects shall be notified through information publicly disclosed in a locally customary manner, or similar actions shall be taken to ensure that the Data Subjects are informed in a similarly effective manner.

If the Enterprise has not yet communicated the data protection incident to the Data Subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may order the notification of the Data Subject, or may decide that any of the above conditions are met, therefore, that informing the Data Subject is not necessary.

7. Data processing registrations

7.1 Registration of data processing

The Enterprise and the representative of the Enterprise shall keep written registration – also including electronic documents – about the data processing activities carried out within its scope of responsibility, under Article 30 of the GDPR, containing the following information:

- The name and contact details of the Enterprise and, where applicable, the joint controller, the controller's representative and the data protection officer,
- Purposes of data processing,
- Description of the categories of Data Subjects and of the categories of personal data,
- The categories of recipients to whom the personal data have been or will be disclosed, including recipients in third countries or international organizations,
- 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 sub-paragraph of Article 49 (1) of the GDPR, the documentation of suitable safeguards,
- Where possible, the envisaged time limits for erasure of the different categories of data,
- Where possible, a general description of the technical and organisational measures referred to in Article 32 (1) of the GDPR.

The Enterprise and the representative of the Enterprise shall make the registration accessible to the supervisory authority upon request.

It is not obligatory to register the data processing activities if the Enterprise employs fewer than 250 persons.

7.2. Registering data protection incidents

The Enterprise registers the following data protection incidents with the following information:

- Facts related to the data protection incident,
- Its impacts and
- Measures made for remedy.

The supervisory authority may access this registration and may check the observation of the provisions of Article 33 of the GDPR.

8. Data Protection Officer

The Enterprise appoints no data protection officer.

9. Data protection impact study

Upon the data protection impact study, the Enterprise shall carry out an impact study into the rights and freedoms of natural persons in the case of data processing activities that presumably carry a high risk. The impact study contains the following data as a minimum:

- a systematic description of the envisaged processing operations and the purposes of processing, including, where applicable, the legitimate interest pursued by the controller,
- an assessment of the necessity and proportionality of the processing operations in relation to the purposes,

- the risks to the rights and freedoms of Data Subjects,
- 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. Effect and order of revision

This Privacy Policy comes into effect on 25 May 2018 and is in effect until revoked. Upon the entry into effect of this Privacy Policy, all formerly effective internal regulations or employer instructions shall lapse under which the Enterprise processed the personal data pertaining to the effect of the Privacy Policy. This Privacy Policy shall be revised at least once a year, on or before the anniversary of its entry into effect.

Dated: Budapest, 25 May 2018