PRIVACY POLICY

- **Introduction**

- Inthera Korlátolt Felelősségű Társaság / Inthera Ltd. / Inthera GmbH

Registered seat: H-1112 Budapest, Eper utca 48/A
Branch office: H-2151 Fót, Külterület utca 0221/12. A1. ép.
Company registration number: 01-09-161471
VAT number: 10647563-2-43
Phone: +36 (1) 400 6746
Email: inthera@inthera.net
Website: www.inthera.net

as a Data Controller (hereinafter referred to as: Company (or Data Controller) shall act in accordance with this Privacy Policy (hereinafter referred to as: Policy), and, in cases not regulated herein, in compliance with Act CXII of 2011 on Informational Self-Determination and Freedom of Information (hereinafter referred to as: Privacy Act) and Regulation (EU) 2016/679 of the European Parliament and of the Council (GDPR).

- The Policy shall be reviewed and amended by the Company at pre-defined intervals in order to ensure compliance with prevailing privacy and other requirements of law.

- Information on the Policy shall be provided by the Company in electronic format, which information can be requested at the aforementioned e-mail address.

- Personal data shall be processed by the Company in compliance with the provisions of the Privacy Act and all relevant measures shall be taken to safeguard such information.

- The Policy contains the information that constituted the basis for providing clear, intelligible and detailed information to data subjects, in particular on the purposes and legal basis of data processing, the data controller and data processor, the duration of data processing, the rights of data subjects and judicial remedies available.

- **Explanatory notes**

    - data subject: a natural person who can be identified, directly or indirectly, in particular by reference to any personal data;
    - personal data: any information relating to a data subject, in particular an identifier such as a name, an identification number, one or more factors specific to the physical, physiological, mental, economic, cultural or social identity of that data subject, as well as any consequence that may be drawn from such data relating to the data subject;
    - special data:
        - personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and data concerning a natural person's sex life;
        - personal data concerning health, addictions or criminal record;
    - Consent of the data subject: any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she,

signifies full agreement to the processing of personal data relating to him or her or restricted to certain operations; Such consent is also deemed to have been given when the data subject puts a check mark in a relevant box on a website, makes the relevant technical settings when using information society related services, as well as makes any other statement or act which, in the relevant context, clearly indicates the data subject's consent to the intended processing of his personal data. Silence, putting a check mark in a box in advance, or non-action therefore does not constitute consent. Consent shall extend to all processing activities performed for the same purpose or purposes. If the processing serves more than one purpose, consent shall be given for all the processing purposes. If consent is given following an electronic request by the data subject, the request shall be clear and concise and shall not unnecessarily prevent the use of services that require consent to be granted.

- objection: a statement of the data subject where he or she objects to the processing of his or her personal data and requests the termination of processing or the erasure of processed data;
- data controller: a natural or legal person or unincorporated organisation that, either alone or jointly with others, defines the intended purposes of data processing, makes and implements decisions regarding the processing of personal data (including the tools used) or engages a data processor to perform such activities.
- data processing: any operation or set of operations performed on the data, regardless of the procedure used, such as collection, recording, organisation, storage, alteration, use, query, transfer, disclosure, alignment or combination, blocking, erasure and destruction, as well as prevention of further use of the data, taking photographs, audio or video recordings, and recording physical characteristics that can be used to identify a person (e.g. fingerprints, palm prints, DNA samples, iris scans);
- data transfer: disclosing data to a specified third party;
- disclosure: making personal data accessible to everyone;
- erasure: making the data unrecognisable in a manner that makes it unrecoverable;
- data marking: the assignment of an identifier to data in order to distinguish it;
- data blocking: the assignment of an identifier to data in order to limit their subsequent processing permanently or for a limited period of time;
- destruction of data: the complete physical destruction of the data storage device, which contains the data;
- data processing: the performance of technical tasks related to data processing operations, regardless of the method and tools used to perform the operations and the place of application, provided that the technical task is performed on the data;
- data processor: a natural or legal person, or unincorporated organisation that processes data on the basis of a contract, including a contract concluded pursuant to a provision of law;
- mandatory Data Protection Officer:

a public authority or other body that performs public duties (regardless of the personal data processed);
its main activity is the extensive, regular and systematic monitoring of data subjects;
or processes large amounts of sensitive or criminal data according to its main activity.

- sets of personal data: sets of personal data processed in a register;
- automated set of personal data: a set of personal data processed automatically;

- automatic processing: includes the following operations, if they are performed in whole or in part by automated tools: data storage, logical or arithmetical operations on data, alteration, erasure, retrieval and dissemination of data;
- user: a natural person who browses the Company's website (www.inthera.net) or sends a message to the Company through the internal mailing system - under “Kapcsolat” / “Contact”;
- third party: any natural or legal person or unincorporated organisation other than the data subject, the data controller or the data processor;
- third country: any state that is not an EEA country;
- personal data breach: unlawful processing of personal data, in particular unauthorised access to, or alteration, transfer, disclosure, erasure, destruction as well as accidental destruction of or damage to personal data.

- **Purpose, scope, principles and legal basis of the Privacy Policy**

  - The processing of data is based on the voluntary, duly informed consent of the users of the content of www.inthera.net that contains the express consent of the Users to the use of their personal data provided during the use of the website. The legal basis for data processing is the voluntary consent provided by the data subject pursuant to Section 5, paragraph (1), item a) of Act CXII of 2011 on Informational Self-Determination and Freedom of Information. Consent is given by the Data Subject in relation to certain processing of his or her personal data by using the Website or by voluntarily providing the relevant data.

  - Description of data processing: The www.inthera.net Website is operated by the Data Controller. The Website is accessible to all and does not require registration or the provision of any data. If the Data Controller inserts a contact form on the Website, the data subject may provide data by filling it in, and the Data Controller will use the data to contact the data subject.

  - The purpose of this Policy and data processing is to:

- lay down the privacy and data processing principles applied by the www.inthera.net Website (hereinafter referred to as Website) operated by the Data Controller and the Data Controller's privacy and data processing policy, which the Data Controller acknowledges as binding on itself;
- specify the procedures for the management of manual or computer-based records that contain personal data and are kept by the Data Controller and provide data for human resources activities;
- ensure compliance with constitutional privacy principles, the requirements of data security, Hungarian laws and the relevant European Union regulation;
- effectively prevent unauthorised access to, alteration of, or unauthorised disclosure of personal data processed by the Data Controller.
- identify the data subject, contact and communicate with the data subject;
- prepare and perform services and contracts;
- fulfill obligations provided for by law.

  - This Policy also aims to ensure that all individuals, irrespective of their nationality or place of residence, are guaranteed in all areas of the services provided by the Company that their rights and fundamental freedoms, in

particular their right to privacy, are respected when their personal data are processed by automated means (privacy).

- Automatically collected data are used to ensure the provision of services available through the Company's websites, to display customised content and advertisements, to compile statistics, the technical development of the IT system and to protect the rights of users. The Data Controller shall be entitled to use the data provided by Users when using the service to form user groups and to display targeted content and/or advertisements to the user groups on the Company's website.

- The Data Controller will process the personal data of visitors to the Website and users of the Company's services in the course of the operation of the Website (personal scope).

- The substantive scope of this Policy covers all processing of personal data (both computerised and manual) performed under this Policy.

- The Data Controller does not verify the personal data received. The accuracy of personal data shall be the sole liability of the person who provides such data. By providing an e-mail address, the User also assumes responsibility for ensuring that he or she is the exclusive user of the e-mail address provided. The assumption of liability means that any liability in connection with access to the Website using a particular e-mail address shall be borne solely by the user who registered by that e-mail address.

- The Data Controller shall observe the following principles in the course of all data processing operations:
    - it shall process personal data only for predefined purposes (purpose limitation principle);
    - it shall process personal data only until the intended purpose of processing is achieved (storage limitation principle);
    - it shall process personal data only to the extent absolutely necessary for the achievement of the intended purpose (data minimisation and data protection by default);
    - data processing shall comply with the requirement of fairness (principle of fairness);
    - data processing shall be lawful (possess an appropriate legal basis);
    - data processed shall be accurate and complete (accuracy principle);
    - data processing shall be based on appropriate, clear, detailed, complete, easily accessible preliminary information (preliminary information principle);
    - data subjects shall be informed about the processing of their data upon request;
    - data subjects may object to the processing of their personal data (right to object), request the erasure of their personal data (right to be forgotten), rectification and blocking of their personal data;
    - the Data Controller shall ensure data security (privacy by design principle),
    - the Data Controller is obliged to record, notify and report any personal data breaches to the authorities (management of personal data breach).

- Personal data may only be processed for specific purposes, for exercising rights and complying with obligations. All phases of processing shall comply with the intended purposes of data processing, recording of personal data shall be fair and lawful.

- Only personal data required for the purpose of data processing and is suitable for achieving that purpose may be processed. Personal data may be processed only to the extent and for the duration required for the purposes they are collected for.

- In all cases when the Company intends to use the personal data provided for purposes other than those intended by the original data collection, the Company shall inform the User thereof and obtain his or her prior explicit consent or provide him or her with the possibility to prohibit such use.

- The personal data will retain this quality during data processing as long as its link to the data subject can be restored. A link can be restored with the data subject, if the Company has the technical requirements needed for restoration.

- The accuracy, completeness, and, if necessary for the purposes of the data processing, the up-to-date nature of data shall be ensured, and the data subject shall be identified only for the time required for the purposes of processing.

- The provision of personal data processed by the Company is voluntary. Certain data forms used by the Company are filled in and returned to the Company by individuals acting under their own responsibility and by granting their consent to the Policy, and the Company processes the personal data thus provided with the consent of the data subjects.
- The data subject may withdraw his or her consent at any time, however, withdrawal shall not affect the lawfulness of the data processing based on consent prior to the withdrawal.

- Personal data may solely be processed
- with the consent of the data subject (Section 5, paragraph (1), item a) of the Privacy Act);
- if processing is required by law, or, on the basis of the authorisation granted by law within the scope specified therein, by a regulation of a local government for purposes in the public interest (hereinafter referred to as: mandatory data processing, Section 6, paragraph (1), item a) of the Privacy Act.);
- if processing is required for the fulfillment of a legal obligation applicable to the Company (Section 6, paragraph (1), item a) of the Privacy Act);
- if processing is required for the purposes of enforcing the legitimate interests of the Company or a third party, and the enforcement of these interests is proportionate to the restriction of the right to the protection of personal data (Section 6, paragraph (1), item b) of the Privacy Act).

- Special data can be processed based on Section 5, paragraph (2) of the Privacy Act.

- The validity of a legal declaration of consent by a minor aged 16 or older to the

processing of his personal data does not require the consent or subsequent approval of his legal representative.

- If the purpose of the processing based on consent is the performance of a contract or a specific statement concluded with the Company, the contract or statement shall contain all the information that the data subject needs to know for the purposes of processing personal data under this Act, in particular the description of the data to be processed, the duration of the processing, the purposes of the processing, the fact of data transfer, the recipients, the fact of engaging a data processor.

- Unless otherwise provided for by law, if personal data have been collected with the consent of the data subject, the Company may process the collected data for the purpose of compliance with a legal obligation of the Company, or for the purposes of a legitimate interest pursued by the Company or a third party, if such interest is proportionate to the restriction of the right to the protection of personal data, without further specific consent and even after the withdrawal of the consent granted by the data subject.

- The Company will transfer personal data to third parties with the consent of the data subjects, and will only link them to other third parties in exceptional cases and only if the data subjects consent thereto, or if such transfer is permitted by law and if the conditions for processing are met for each personal data respectively.

- The Company does not transfer personal data to a data controller or data processor located in a third country.

- If the retention, or transfer of certain data provided is required by law, the data subjects shall be notified of such disclosure through the contact details they have provided.

- **Types of data recorded, method and duration of data processing**

  - The User provides the following data when contacting the Company over the Website, when expressing interest about the Company's services and in order to communicate with the Company:

- name
- e-mail address
- telephone number
- company name
- address
- position
- message text

The Company processes the personal data of natural persons who contact it for the purposes of requesting a price quotation, submitting a quotation or performing a contract for the period required for the performance of the contract. The legal basis of data processing by the Company is the performance of the contract, the purpose of data processing is to communicate with the natural

person as a contracting party, the assertion of claims arising out of the contract and the fulfillment of obligations arising out of the contract. The Company shall process the personal data of natural persons contracted for the period specified by the provisions of law that require the retention of the contract.

- Processing of personal data related to employment

- Processing of personal data prior to employment

The Company processes personal data required to perform a recruitment procedure related to the applications for the advertised position, the assessment of the suitability of candidates for the job prior to the establishment of the employment. The legal basis for data processing is the consent granted by the natural person who submitted the application. The purpose of data processing is to assess the candidate's application, determine his or her suitability for the job and conclude an employment contract. In addition to the candidate's personal identification data (name, name at birth, date and place of birth, mother's name at birth, address), the Company processes personal data required to assess the candidate's suitability for the position (education, studies, expertise, previous work experience), communication (telephone number, e-mail address) and the candidate's photograph. Once the employee has been selected, the purpose of data processing ceases to apply to other candidates who are not selected, and the personal data of the unselected candidates shall be erased immediately. The purpose of processing personal data of applicants who withdraw their applications before the assessment thereof ceases to exist at the moment of withdrawal of the application and therefore their personal data shall be erased without delay. The candidate shall be informed of the outcome of the assessment of their application. The Company will not be obliged to erase personal data, if the applicant expressly consents to the Company's continued processing of his or her personal data for the purpose of receiving notifications of future job opportunities following an unsuccessful application.

- Processing of personal data during employment

The Company processes the personal data of its employees that are recorded in the payroll record. Such personal data includes the followings: name; mother's name at birth; address, place of stay, notification address; contact details (telephone number, e-mail address); social security number, tax identification number, type and number of personal identity document; amount of salary; name of their bank and bank account number; the amount and title of deductions and withholdings from the salary and the bank account number of the person entitled to receive the deductions and withholdings; the names and social security numbers of children and dependants; the name and contact details of the closest relative to be notified.
Purpose of data processing: the performance of obligations and exercising rights arising out of an employment, the establishment and termination of an employment.
Duration of data processing: the duration of the employment and 8 years after the termination of the employment or, if the latter is longer, for the period specified by law.
Legal basis for processing: legitimate interest of the employer, performance of a legal obligation, performance of an employment contract. The employee shall be informed of the legal basis and the purposes of the data processing before the processing starts.

- Data technically recorded during the operation of the system: the data of the User's computer used for logging in, which are generated during the use of the service and which are recorded by the Data Controller's system as an automatic result of technical processes. Data automatically recorded is automatically logged by the system upon logging in or out, without any additional declaration or action by the User. Such data cannot be linked to other personal data of the users, except in cases when required by law. Data are only accessible to the Data Controller.

- Cookie:

To provide you with a customised service, the Company's website uses anonymous user

identifiers, so-called “cookies”. A cookie is a series of signals, information files that are placed on a user's computer by service providers to allow a website to record information about a user's browsing habits (for example, store a user's preferences and settings; help them to log in; display customised ads and analyse the functioning of the website). However, the series of signals stored in a cookie is only capable of recognising the user's computer and is not suitable to identify the user individually.
The Data Controller uses Google Tag manager, Google Analytics, Google Ads, Facebook Pixel and Linkedin cookies to collect information about how Users use the Website. These cookies collect data for remarketing, statistics and conversion measurement purposes, and are not suitable to identify the User personally (the IP address used is only partially recorded), they collect information such as the pages viewed, the part of the Website clicked on, the number of pages visited, the length of time spent in each session, the potential error messages received, all aimed at improving the Website and the user experience. The legal basis for the processing of such cookies is the consent of the User. The purpose of the processing is for the Data Controller to collect information about how Users use the Website. Duration of data processing related to cookies shall be 30 days.
All modern browsers allow you to customise your cookie settings. Most browsers automatically accept cookies by default, however, such cookie settings can usually be changed to prevent automatic acceptance thereof, and allow you to choose each time whether you as a User intend to allow cookies or not.

- The User has the opportunity to request information from the Company on the processing of his or her personal data as specified in Chapter VII of the Policy.

- Transfer of personal data to third parties: The Controller may only transfer data to third parties who are required to be involved in the performance of the Company's obligations (suppliers required to perform contracts, insurance companies, third parties required to perform employee-related obligations, e.g. accountants.)

- The Company's system may collect data on user activity, however, such data cannot be linked to data generated by Users when using other websites or services.

- **Period of data processing**

    - Personal data provided by the User will be processed until the User unsubscribes from the service with the given user name. The date of erasure shall be 10 business days upon the date of receipt of the User's request for erasure. In case of unlawful or misleading use of personal data, or in case of a criminal offence or system attack committed by the User, the Data Controller shall be entitled to erase the User's data without delay, and in case of suspected criminal offence or civil liability, the Data Controller shall be entitled to retain the personal data for the duration of future proceedings.

    - Personal data provided by the User, even if the User fails to unsubscribe from the services, may be processed by the Company as Data Controller until the User explicitly requests the termination of their processing in writing. The User's right to use the service shall not be affected by his or her request to terminate processing of his or her personal data without unsubscribing from the service. Personal data will be erased within 10 business days upon receipt of the relevant request.

- Data which are automatically, technically recorded during the operation of the system are stored in the system for a period of time from their generation that is reasonable to ensure the operation of the system. The Company shall ensure that these automatically recorded data cannot be linked to other personal data of the users, except in cases when required by law. If the User has withdrawn his or her consent to the processing of his or her personal data or has unsubscribed from the service, his or her identity will no longer be identifiable from the technical data.

- **Data security requirements**

  - The Company is obliged to design and implement data processing operations in a manner to ensure the protection of the privacy of data subjects upon applying the Privacy Act and other rules related to processing of personal data.

  - The Company, or, in the scope of its activities, the data processor, shall be obliged to ensure the security of the data, and shall also be obliged to take technical and organisational measures and to establish procedural rules required to enforce the Privacy Act and other privacy and confidentiality rules.

  - Appropriate measures shall be taken to protect personal data against, in particular, unauthorised access, alteration, transfer, disclosure, erasure or destruction, accidental destruction or damage and inaccessibility caused by changes in the technology applied.

  - In order to protect the data files processed electronically in different registers, appropriate technical measures should be taken to ensure that the data stored in the registers cannot be directly linked and assigned to data subjects unless permitted by law.

  - When processing personal data by automated means, the Company and the data processor shall take additional measures to ensure that

- unauthorised data entry is prevented;
- use of an automated data processing system by unauthorised persons and data transfer equipment is prevented;
- it is verifiable and ascertainable, which organisations received or may receive personal data through data transfer equipment;
- it is verifiable and ascertainable, which personal data have been entered into automated data processing systems, when and by whom;
- the installed systems can be restored in case of an interruption, and
- error reports are generated on automated processing.

  - The Company and the data processor shall take into consideration the prevailing level of technology available when defining and applying data security measures. If there are several possible data processing solutions, the one that provides the highest protection of personal data should be chosen, unless that would impose a disproportionate burden on the Company.

- **Rights of data subjects and assertion thereof**

  - The data subject may request the Company to inform him or her about the processing of his or her personal data, to rectify his or her personal data, and to erase or block his or her personal data, except for the cases of mandatory data processing.

  - The Company shall provide information on the data subject's personal data processed by the Company, or by a data processor appointed by the Company on the source of data, the purpose, legal basis and duration of processing, the name and address of the Data Processor and its activities related to processing, the circumstances of the personal data breach, its impact and the measures taken to remedy the personal data breach, and, in the case of transfer of personal data, the legal basis and the recipient of the transfer.

  - The Company shall, if it has an internal data protection officer, through the internal data protection officer, keep a register for the purpose of monitoring the measures taken in relation to the personal data breach and informing the data subject, which shall include the scope of the personal data concerned, the number and type of data subjects affected by the personal data breach, the date, circumstances, effects and measures taken to remedy the personal data breach, and other data specified in the legislation that requires processing.

  - The duration of the obligation to retain data in the aforementioned registers, and therefore, to provide information may be limited by the law that provides for data processing. A period of less than five years may not be specified under this limitation in the case of personal data and twenty years in the case of special categories of personal data.

  - The Company shall provide the information in writing in an intelligible form within the shortest possible time from the date of the request, but not later than 25 days, upon the request of the data subject, which information shall be free of charge if the person requesting the information has not yet submitted a request for information to the Company for the same data in the current year. In other cases, reimbursement of costs may be granted. The amount of the reimbursement may also be specified in a contract concluded by and between the parties. Reimbursement of costs already paid shall be repaid, if data have been unlawfully processed, or if the request for information has led to a rectification.

  - The Company may refuse to provide the data subject with information only in cases specified in Section 9, paragraph (1) and Section 19 of the Privacy Act.

  - In case the Company refuses to provide information, it shall notify the data subject in writing which provision of the Privacy Act constitutes the basis for the refusal. In case the Company refuses to provide information, it shall notify the data subject of the possibility of bringing a claim or lodging a complaint with the Hungarian National Authority for Data Protection and Freedom of Information (hereinafter referred to as: Authority).

  - The Company shall notify the Authority of rejected requests until 31 January

each year following the particular year.

- If the personal data is not accurate and accurate personal data is available to the Data Controller, the Data Controller shall rectify the personal data.

- Personal data shall be erased if processing is unlawful; erasure is requested by the data subject; data is incomplete or inaccurate, and this status cannot be lawfully remedied, provided that erasure is not excluded by law; the purpose of processing has ceased, or the retention period provided for by law has expired; erasure has been ordered by a court or the Authority.

- If so requested by the data subject, or if based on available information it can be assumed that erasure would violate the legitimate interest of the data subject, the Company shall block personal data instead of erasing it. Blocked personal data may only be processed until the purpose of processing that hindered erasure of the personal data persists.

- The Company shall mark the personal data processed, if the data subject contests the accuracy or correct nature of such personal data, but the inaccuracy or incorrectness of the contested personal data cannot be clearly ascertained.

- The data subject and any data processor, who had been a recipient of such data transfer shall be notified of any and all rectification, blocking, marking and erasure. Notification may be disregarded if this does not harm the legitimate interests of the data subject in relation to the purpose of processing.

- If the Company fails to comply with the data subject's request for rectification, blocking or erasure, it shall provide written reasons for refusing the request for rectification, blocking or erasure indicating the facts and legal background thereof within 25 days upon receipt of the request. In case the Company rejects the request related to rectification, erasure or blocking, it shall notify the data subject of the possibility of bringing a claim or lodging a complaint with the Authority.

- The rights of the data subject specified above may be restricted by the law for the purposes of the external and internal security of the State, such as defence, national security, the prevention or prosecution of criminal offences, the security of law enforcement, or for reasons of economic or financial interest of the State, a local government, important economic or financial interests of the European Union, and for the purpose of preventing and investigating disciplinary or ethical offences, breach of employment rights and occupational health and safety obligations associated with the exercise of professional activities, including in all cases control and supervision, and the protection of the rights of the data subject or others.

- The data subject shall be informed before the processing starts whether the processing is based on his or her consent, or is mandatory.

- The data subject shall be informed clearly and in detail of all the facts relating to the processing of his or her personal data, in particular the purposes and

legal basis of data processing, the identity of the data controller and data processor, the duration of data processing and the persons who may access the data, before data processing is started. The information should also cover the rights and remedies available to the data subject in association with the processing.

- The data subject shall be entitled to object to the processing of his or her personal data;

- where the processing or transfer of personal data is necessary for the fulfillment of a legal obligation to which the Company is subject or for the purposes of the legitimate interests pursued by the Company, the data subject or a third party, except in the case of mandatory data processing;
- if the personal data are used or transferred for direct marketing, public opinion polls or scientific research purposes; and
- in other cases specified by law.

- The Company shall assess the objection as soon as possible, but not later than within 15 days of the submission of the request, and shall decide whether the objection is justified and inform the applicant of its decision in writing.

- If the objection of the data subject is found to be justified by the Company, it shall terminate the processing of personal data, including any further collection and transmission, and shall block the data, as well as notify all persons to whom the personal data concerned by the objection were previously disclosed of the objection and who are obliged to take measures to enforce the right to object.

- If the data subject is dissatisfied with the Company's decision, or if the Company fails to comply with the deadline, the data subject may bring a claim within 30 days of the notification of the decision or the last day of the deadline.

- If the recipient of data does not receive the data required to exercise its rights due to an objection by the data subject, the Company may bring a claim against the data subject within 15 days upon the notification of the objection, if the objection is justified, in order to obtain access to the data. The Company may also interplead the data subject.

- If the Company fails to give notice when the objection is justified, the recipient of data may request clarification from the Company on the circumstances relating to the failure to transfer the data, which clarification shall be provided by the Company within 8 days upon the delivery of the recipient's request. In case of a request for clarification, the data subject may bring a claim against the Company within 15 days upon the provision of the clarification, but not later than the deadline specified for such claims. The Company may also interplead the data subject.

- The Data Controller shall not be entitled to erase personal data if processing of personal data is required by law. However, personal data may not be transferred to the recipient thereof if the Company consented to the objection, or if the objection was found justified by court.

- **Remedies before courts and authorities**

    - The data subject may bring a claim against the data controller in case of a breach of his or her rights or in other cases. The court shall act on the case without delay.

    - The Company is obliged to prove that the data processing complies with the provisions of the law.

    - The data subject may also, at his or her option, bring a claim before a court having jurisdiction over his place of residence or stay.

    - A person who does not otherwise have full legal capacity can also become a party to the action. The National Authority for Data Protection and Freedom of Information shall be entitled to intervene in the action in order to ensure that the data subject wins.

    - If the court upholds the action of the data subject, the Company may be obliged by the court to provide the information, rectify, block or erase data, destruct any decision made by automated data processing, take into consideration the right of the data subject to object to the processing of his or her personal data, or provide the data requested by the data subject.

    - If the data subject's request is rejected by the court, the Company shall be obliged to erase personal data related to the data subject within 3 days upon the announcement of the judgment. The Company shall also be obliged to erase the personal data, if the data subject fails to bring a claim within the available deadline.

    - The court may order the disclosure of its judgment by publishing the identification data of the Company, if the interests of data protection and the rights of a larger number of data subjects protected under this law require such actions.

    - Any person may submit a notification to the Authority to initiate an investigation claiming that there is a breach or imminent threat of a breach of rights relating to the processing of personal data or the exercise of rights of access to data of or in the public interest.

    - Nobody can become disadvantaged due to filing a claim with an Authority. The identity of the announcer may only be disclosed by the Authority, if the investigation could not be performed without such disclosure. The identity of the announcer may not be disclosed by the Authority if non-disclosure is requested by the announcer, even if the investigation cannot be performed without such disclosure. The Authority shall inform the announcer of such consequences.

    - The investigation conducted by the Authority shall be free of charge and the costs of the investigation shall be paid in advance and be borne by the Authority.

- Contact details of the Authority:

Hungarian National Authority for Data Protection and Freedom of Information

Address: H-1055 Budapest, Falk Miksa u. 9-11.
Mailing address: H-1363 Budapest, Pf.: 9.
Phone: +36 (30) 683-5969, +36 (30) 549-6838, +36 (1) 391 1400
Email: ugyfelszolgalat@naih.hu
URL: http://naih.hu

- **Damages and compensation:**

  - The Company shall be liable to compensate any and all damage caused to others by the unlawful processing of the data subject's personal data or by violating the requirements of data security.

  - The data subject shall be entitled to claim compensation from the Company, if his or her rights of the personality are violated by the Company by unlawfully processing his or her data or by violating the requirements of data security.

  - The Company shall be liable to the data subject for any damage caused by the Data Processor, and the Company shall also be liable to pay compensation to the data subject for any violation of the rights of the personality caused by the Data Processor.

  - The Company shall be exempted from liability to pay compensation for the damage caused, if it can justify that the damage or the violation of the data subject's rights of the personality was caused by an inevitable cause outside the scope of data processing.

  - No compensation may be claimed and no compensation for damage shall be paid if the damage or the violation of the rights of the personality was caused by the party who incurred the damage or the intentional or grossly negligent behaviour of the data subject.

- **Miscellaneous data processing**

  - If data are collected for a reason not specified in the Policy, the data subjects will be informed thereof upon the collection of their personal data.

  - In special cases, the Company is obliged to provide information, disclose and hand over data as well as documents upon request to courts, prosecutors, investigating authorities, law enforcement authorities, administrative authorities, the National Authority for Data Protection and Freedom of Information, or other bodies authorised by law. In such cases, the Company will disclose the personal data to the requesting authority only to the extent strictly required for the purpose of the request (if the specific purpose and scope of the data have been specified).

- **Scope of the Policy:**

- This Policy shall enter into force and effect on the day of its disclosure and shall remain in force and effect until revoked. The Company reserves the right to amend this Policy unilaterally based on laws, EU regulations and case law.

- All Users shall be informed appropriately after any amendment to the Privacy Policy. Users acknowledge the amended data processing rules by the continued use of the services, and no further user consent is required.

Effective as of 2024