ECCONSTECH LTD. PRIVACY NOTICE

Ecconstech Ltd. (hereinafter: "Data Controller") pays special attention to the protection of personal data during its activities, compliance with mandatory legal provisions, and safe and fair data handling. The Data Controller considers it important to respect and enforce the data protection rights of any natural person who comes into contact with it in any way (hereinafter: "Data Subject"). Therefore, the Data Controller undertakes to ensure that its data processing related to its activities and services complies with the requirements set out in this Notice and applicable laws.

In view of the above, the Data Controller creates the following privacy notice (hereinafter: "Privacy Notice", "Notice") for the purpose of ensuring the lawfulness of its internal data processing processes, maintaining records, and ensuring the rights of data subjects.

Data Controller's name: Ecconstech Information Technology Limited Liability Company
Data Controller's company registration number: 13-09-209758
Data Controller's tax number: 28980771-2-13
Data Controller's registered office: 2030 Érd, Kossuth Lajos street 150.
Data Controller's representative name: Péter István Szemesy, managing director
Representative's contact: peter.szemesy@eccons.tech

PART I: GENERAL PRINCIPLES

Purpose of the Notice

By creating and making available this Notice, the Data Controller intends to ensure the realization of the right to information of data subjects as defined in Articles 13-14 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter: "GDPR" or "Regulation"). The purpose of the Notice is to ensure that the Data Controller complies with the provisions of the GDPR and Hungarian legislation affecting the processing of personal data, in particular the provisions of Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information (hereinafter: "Info Act").

The Privacy Notice establishes the legal framework for data processing at the Data Controller, ensures the enforcement of constitutional principles of data protection and the right to informational self-determination, facilitates compliance with data security requirements, and prevents unauthorized data processing, establishes tasks and responsibilities important from a data protection perspective in data security. The purpose of the Notice is furthermore to establish and operate a protection system for personal data processed by the Data Controller in its capacity as data controller or data processor.

The purpose of this Notice is also to ensure that data subjects receive appropriate information about the data processed by the Data Controller and any data processors commissioned by the Data Controller, their sources, the purpose, legal basis, and duration of data processing, the name and address of any data processor involved in the data processing and their activities related to data processing, - in case of transfer of the data subject's personal data - the legal basis and recipient of the data transfer, as well as

the rights of the data subject.

Personal data processed by the Data Controller must be protected in particular against unauthorized access, alteration, transmission, disclosure, deletion or destruction, accidental destruction and damage, as well as becoming inaccessible due to changes in the applied technology. To protect electronically processed data files, appropriate technical solutions must ensure that the data processed in the registers - unless permitted by law - cannot be directly connected and assigned to the data subject.

The current version of the Privacy Notice is always available at the Data Controller's registered office. This Notice is effective from May 15, 2024.

Applicable Legislation

The Notice shall be applied in accordance with the following legislation:
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter: "GDPR")
- Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information (hereinafter: "Info Act")
- Act V of 2013 on the Civil Code (hereinafter: "Civil Code").

Definitions

- Data subject: any identified or identifiable natural person based on personal data.
- 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 category data: all data belonging to special categories of personal data, namely personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as 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.
- Consent: any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
- Objection: a statement by the data subject objecting to the processing of his or her personal data and requesting the cessation of processing or deletion of the processed data.
- Data controller: the natural or legal person, or organization without legal personality, which, alone or jointly with others, determines the purposes of data processing, makes and executes decisions regarding data processing (including the tools used), or has them executed by the data processor.
- Data processing: any operation or set of operations performed on data regardless of the procedure used, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction, as well as preventing further use of the data, taking photographs, sound or video recordings, as well as recording physical characteristics suitable for identifying a person (e.g., fingerprints, palm prints, DNA samples, iris images).

- Data transfer: making data available to a specific third party, disclosure: making data available to anyone.
- Data processing: performing technical tasks related to data processing operations, regardless of the method and tools used to perform the operations, as well as the place of application, provided that the technical task is performed on the data.
- Data processor: a natural or legal person, or organization without legal personality, which processes data on the basis of a contract - including contracts concluded on the basis of legal provisions.
- Third party: a natural or legal person, or organization without legal personality, which is not identical with the data subject, the Data Controller or the data processor.
- Recipient: a natural or legal person, public authority, agency or any other body to whom or which personal data are disclosed, whether a third party or not. Public authorities which may have access to 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 comply with the applicable data protection rules according to the purposes of the processing.
- Personal data breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Data Controller's Data Processing Principles and Rules

- In accordance with the principles of lawfulness, fairness and transparency, the Data Controller processes personal data lawfully and fairly, and in a transparent manner for the data subject, in order to exercise a right or fulfill an obligation. The Data Controller strictly prohibits the use of personal data it processes for private purposes.
- In accordance with the principle of purpose limitation, the Data Controller collects and processes personal data only for specified, explicit and lawful purposes, to the minimum extent and for the time necessary to achieve the purpose, and does not process them in a manner incompatible with those purposes. Accordingly, the Data Controller uses the personal data of data subjects exclusively for the purposes communicated at the time of collection or for other appropriate purposes in accordance with the law.
The Data Controller pays special attention to ensuring that its data processing always complies with the principle of purpose limitation, and if the purpose of data processing has ceased or the data processing is otherwise unlawful, the data will be deleted. If personal data is no longer needed, it must be destroyed securely and documented.
- In accordance with the principle of data quality (data minimization and accuracy), the Data Controller only processes and collects the amount of personal data that is appropriate, relevant and necessary for the purposes of data processing. The Data Controller also takes reasonable measures to ensure that personal data is accurate, complete and up-to-date, and that personal data unnecessary for data processing purposes is deleted.
- In accordance with the principle of storage limitation, the Data Controller processes personal data enabling the identification of data subjects only for the period necessary to achieve the purposes of data processing. Following the change or cessation of the data processing purpose, the Data Controller ensures the deletion of the data. The Data Controller stores personal data for a longer period only if the personal data is processed for public interest archiving purposes, for scientific and historical research purposes or for statistical purposes. Special care is taken when disposing of data carriers containing personal data.
- In accordance with the principle of integrity and confidentiality, the Data Controller ensures closed,

comprehensive, continuous and risk-proportionate protection of personal data, takes organizational and technical measures particularly to establish protection against unauthorized or unlawful processing of data, accidental loss, destruction or damage. To protect data against unauthorized use or disclosure, the Data Controller applies data security controls in its own activities.
The information security measures designed and implemented by the Data Controller ensure the confidentiality, integrity and availability of personal data.
- In accordance with the principle of accountability, the Data Controller plans and executes its data processing processes and designs its data processing system in such a way that it is able to demonstrate compliance with the principles set out in this point at any time during data processing, in particular when, in what form the personal data was collected and what information the data subject received when the personal data was collected.

Data Security Rules

The Data Controller ensures the highest level of security reasonably expected for personal data processed throughout the data processing. The Data Controller performs its data processing operations in such a way as to ensure appropriate security of personal data through the application of appropriate technical and organizational measures, including protection against unauthorized or unlawful processing of data, accidental loss, destruction or damage (integrity and confidentiality). The Data Controller also protects personal data with appropriate measures, in particular against unauthorized access, alteration, transmission, disclosure, deletion or destruction, as well as accidental destruction and damage, and against becoming inaccessible due to changes in the technology used.

The Data Controller, taking into account the state of the art and the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, implements appropriate technical and organizational measures to ensure a level of security appropriate to the risk. It ensures data security, takes the technical and organizational measures and establishes the procedural rules necessary for the enforcement of the GDPR and other personal data protection rules.

The Data Controller takes the necessary measures to ensure secure storage of data during the data processing period and final and irreversible deletion and physical destruction of the data set after the expiration of the period.

The Data Controller thus takes the following measures to ensure data security.

1. Personal data processed on paper

To ensure the security of personal data processed on paper, the Data Controller applies the following measures:
- data may only be accessed by authorized persons, others may not have access to it. The Data Controller maintains a register of persons accessing the data;
- Paper-based documents containing personal data are stored by the Data Controller in well-lockable, dry premises, cabinets, and certain documents in separately lockable archives, which only authorized persons may enter.
- If personal data processed on paper is digitized, the Data Controller applies the security rules applicable to digitally stored documents.

- Paper-based data carriers must be deprived of personal data using a document shredder or by using an external company specializing in document destruction.

2. Personal data stored on computers

To ensure the security of personal data stored on computers or networks, the Data Controller applies the following measures and guarantee elements:
- The Data Controller chooses the method of storing data by IT methods in such a way that their deletion - taking into account any different deletion deadlines - can be carried out at the expiration of the data deletion deadline or, if necessary for other reasons.
- If the purpose of data processing has been achieved or the data processing deadline has expired, the file containing the data is irreversibly deleted, the data cannot be recovered.
- The computers used during data processing are owned by the Data Controller or the Data Controller has ownership-equivalent rights over them.
- Documents containing personal data on the computer can only be accessed with valid, personal, identifiable authorization - at least with a username and password - by the authorized person.
- The Data Controller maintains a register of the authorization granted to persons accessing various personal data and the level of authorization.
- It monitors and documents the destruction of electronic data carriers, which it preserves in a retrievable manner.
- Continuously ensures virus protection for IT systems processing personal data.
- Prevents network access by unauthorized persons using passwords on available computing equipment.

The Data Controller also makes security backups of electronically processed personal data.
The Data Controller maintains a data transfer register in which the legality of any data transfer can be verified. The register records the definition of the scope of personal data transferred, the time of data transfer, its legal basis, the recipient of the data transfer, and other data specified in legislation.

The Data Controller prints electronically processed personal data only when this is expressly necessary for exercising a right or fulfilling an obligation.

Management of Data Protection Incidents

In the event of a breach of data security or the accidental or unlawful destruction, loss, alteration, unauthorized transmission or disclosure of personal data processed by the Data Controller, or unauthorized access to them (hereinafter: "data protection incident"), or suspicion of such occurrence, the Data Controller and any person who becomes aware of personal data processed by the Data Controller on any legal basis shall proceed in accordance with this section.

A data protection incident, in the absence of appropriate and timely measures, may cause physical, material or non-material damage to natural persons, including loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorized reversal of pseudonymization, damage to reputation, loss of confidentiality of personal data protected by professional secrecy, or any other significant economic or social disadvantage to the natural person concerned.

The Data Controller therefore handles data protection incidents that come to its attention according to

the following provisions:

1. Detection and reporting of data protection incidents

Data protection incidents and potential sources of danger may be encountered or detected by the Data Controller's employee, contracted partner, person using its services, or its contractor or subcontractor developing, operating and maintaining its IT systems.

When an incident is detected, it is necessary to record and document the characteristics of the incident and all its essential details, take photographs if necessary, and make a copy of the IT device screen.

The Data Controller does not use a template or mandatory form for reporting data protection incidents, but the reporter must, as a general rule, make the report in permanent form (in writing on paper or electronically) to the Managing Director. In case of verbal notification, the Managing Director is obliged to take minutes of the notification, which must contain all available information related to the incident.

Generally, before or during the occurrence of incidents, special human behavior and/or incorrect, unusual operation of the IT system occurs. It is important that in the absence of professional competence, the person detecting the incident should not intervene in the process, should not begin investigating the event on their own authority, or remedying it. Exceptions to this are measures taken to prevent property damage or protect human life.

The Data Controller's employee, subcontractor, or any contractual partner is obliged to report any incident that can be related to information security and/or data protection immediately after becoming aware of it, but no later than within four working hours of becoming aware of it to the Data Controller's Managing Director.

The notification contains the name of the Data Controller, the name and position of the reporter, as well as the subject of the incident, a brief description and whether the incident affects any IT system used by the Data Controller, and whether there is a chance of leakage of personal data of a wider range of data subjects or access by unauthorized persons.

It is also necessary to specifically draw the Managing Director's attention in the notification if the detected data protection incident may not only pose a threat to or cause damage to the Data Controller's IT system, but may also adversely affect the IT system of the Data Controller's contracted partners or cause damage (material or non-material) to these clients.

Following the notification, the Managing Director immediately begins investigating and evaluating the data protection incident and takes all necessary initial steps that are suitable for reducing the extent of damage caused by the data protection incident or preventing the creation of further data protection incidents.

The Managing Director is obliged to immediately notify all of the Data Controller's contracted partners for whom it performs data processing if the incident affects the contracted party's information system and there is a chance of a series of further incidents occurring if notification is not made.

In case of an incident affecting the Data Controller's IT system, the Managing Director is obliged to notify

the person responsible for system operation, who is obliged to assist the Managing Director in investigating the incident.

2. Investigation and evaluation of data protection incidents

The Data Controller's Managing Director - in cooperation with the person responsible for system operation in case of an incident affecting the IT system - examines the notification and, if necessary, requests additional data about the incident from the reporter.

The Managing Director examines the report and, if necessary, requests additional data about the incident from the reporter. The Managing Director may also involve the heads and employees of organizational units (areas) affected by the data protection incident in their work, who are obliged to cooperate with the Managing Director.

The Managing Director is obliged to investigate the following information (if they do not emerge from the report) to the best of their ability:
- the time and place of the data protection incident,
- the scope of data affected by the data protection incident,
- the scope and number of persons affected by the data protection incident.

Upon request, the reporter is obliged to provide the time and place of the data protection incident, other circumstances of the data protection incident, the scope of data affected by the data protection incident, its quantity, the scope and number of persons affected by the data protection incident, the expected effects of the data protection incident, and a list of measures taken to prevent the data protection incident and mitigate its consequences.

The reporter fulfills the data provision immediately, but no later than within 4 working hours.

From this data, the Managing Director prepares a summary of the expected effects of the data protection incident and prepares an action plan to mitigate its consequences. The investigation must be completed within three working days of receipt by the Managing Director at the latest.

The investigation must include whether the data protection incident poses a high risk to the rights and obligations of data subjects, what type of risk is involved, and whether it is necessary to inform data subjects about the incident. If it is not necessary to inform data subjects, the investigation must also include the reasons for this.

The Data Controller evaluates the data protection incident according to the following aspects:
- type of incident (confidentiality, integrity or availability),
- nature of personal data (personal data / special category),
- number of personal data,
- number of affected persons,
- categories of affected natural persons,
- identifiability of affected natural persons,
- likelihood and severity of consequences for the natural person;
- legal basis of the affected data processing

A data protection incident may be classified as risky if the following conditions exist:
- the data affected by the incident includes data falling into special categories of personal data;
- the number of personal data affected by the incident exceeds 100;
- the natural persons affected by the incident include natural persons under 16 years of age;
- the number of natural persons affected by the incident exceeds 100;
- the personal data affected by the incident is suitable for direct contact with the data subject;
- the personal data is suitable for identity theft or fraud of the affected natural person;
- the personal data affected by the incident is capable of causing financial loss to their data subjects.

A data protection incident is likely not to pose a risk if none of the conditions listed above apply or at least one applies, but the Data Controller is able to prove that it has provided the affected personal data with physical and/or IT protection that has not been compromised since the incident occurred.

The Data Controller classifies the data protection incident as likely high risk if at least two of the conditions listed above apply, or at least one applies and the Data Controller is unable to prove that it has provided the affected personal data with physical and/or IT protection that has not been compromised since the incident occurred.

As a result of the investigation, the Data Controller's Managing Director - consulting with the person responsible for IT infrastructure operation if necessary - arranges for the necessary steps to be taken.

3. Register of data protection incidents

The Data Controller's Managing Director maintains a register of data protection incidents. The register contains:
- the scope of affected personal data,
- the scope and number of persons affected by the data protection incident,
- the time of the data protection incident,
- the circumstances of the data protection incident,
- its effects,
- measures taken to remedy it, and
- other data prescribed by law.

The sample register for recording data protection incidents is contained in Annex 8 of this Notice.

4. Notification of data protection incident to the Authority

The Data Controller notifies the Authority of the data protection incident immediately after becoming aware of it, but no later than 72 hours after the Data Controller becomes aware of the incident, unless the incident is unlikely to pose a risk to the rights and freedoms of natural persons. If the notification is not made on time, the Data Controller's Managing Director is obliged to justify the reason to the Authority.

The notification to the Authority must contain:
- the scope and approximate number of data affected by the data protection incident,
- the scope and approximate number of persons affected by the data protection incident,
- the nature and circumstances of the data protection incident,
- the likely consequences of the data protection incident, and

- measures taken to remedy and mitigate the data protection incident.

The Managing Director is responsible for notifying the Authority of data protection incidents.

5. Informing data subjects about data protection incidents

If the data protection incident is likely to pose a high risk to the rights and freedoms of natural persons and it is necessary to inform data subjects, the Data Controller's Managing Director immediately notifies the data subjects. Informing data subjects is independent of the notification obligation to the Authority.

Data subjects need not be informed:
- if the Data Controller has implemented technical, organizational, protective measures on the affected data that prevent access to the data by unauthorized persons or prevent the data from being intelligible;
- if following the data protection incident, the Data Controller has taken measures that ensure that the identified data processing risk is unlikely to materialize;
- if the notification would require disproportionate effort. In this case, data subjects must be informed through publicly disclosed information, which may also be done electronically.

The Managing Director is obliged to inform data subjects.

Exercise of Data Subject Rights

The Data Controller pays special attention to ensuring that the exercise of data subject rights defined in Articles 12-23 of the GDPR complies with legal requirements and data subjects' expectations.

The data subject may request information about the processing of their personal data and is entitled to access the information specified in Article 15 of the GDPR, and may request the rectification of their personal data, or - except for data processing required by law - deletion or restriction of processing, or if the conditions in Article 21 of the GDPR are met, object to the processing of personal data, or exercise the right to data portability or the right to withdraw consent by letter sent to the Data Controller's registered office or in person, and is also entitled to contact the Data Controller's managing director at peter.szemesy@eccons.tech regarding the processing of their personal data.

1. Deadline for fulfilling requests

The Data Controller is obliged to respond in writing, in an understandable form, to the data subject's request regarding the processing of their personal data (when exercising any right) within one month of receipt at the latest. If necessary, taking into account the complexity of the request and the number of requests, this deadline may be extended by a further two months. The Data Controller informs the data subject of the extension of the deadline within one month of receipt of the request, indicating the reasons for the delay.

2. Method of fulfilling requests

The Data Controller strives to ensure that the information provided to the data subject is always concise, transparent, intelligible, easily accessible, clear and understandable, while complying with the rules defined by the GDPR. When a request is submitted to exercise data subject rights, the Managing Director

handles and fulfills the requests or arranges for the fulfillment of requests. The Data Controller provides all information to the data subject in writing as a general rule. If the data subject submitted the request electronically, the information should be provided electronically where possible, unless the data subject requests otherwise.

3. Possibilities for rejecting requests

Taking into account the rules in Article 12(4) and Article 32 of the GDPR (data security), the rights of the data subject - with the exception of the right to general prior information about data processing - can only be exercised if the requester is properly identified and the requirements ensuring authentication of the content of their request are met.

Rights cannot be exercised for requests submitted in a manner that allows limited identification of the requester, particularly:
- not complying with the provisions for private documents with full probative force specified in other legislation, or
- not authenticated with an electronic signature, or
- requests received via email, telephone, or fax.

If identity verification does not occur, the Data Controller is entitled to reject the data subject's request and is obliged to inform the data subject about the method of exercising their rights.

The Data Controller does not accept any form of identity verification by telephone, so the data subject cannot initiate the exercise of their rights by telephone.

4. Information and access

In accordance with the obligation in Article 13 of the GDPR, the Data Controller is obliged - if the personal data originates from the data subject at the time of obtaining the personal data - to make the following information about data processing available to data subjects:
a) the identity and contact details of the data controller and its representative;
b) the contact details of the data protection officer, if any;
c) the purposes of the intended processing of personal data and the legal basis for the processing;
d) where applicable, the recipients of personal data or categories of recipients, if any;
e) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
f) information about the data subject's right to request from the data controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing of such personal data, as well as the right to data portability;
g) where processing is based on consent, the right to withdraw consent at any time, which does not affect the lawfulness of processing based on consent before its withdrawal;
h) the right to lodge a complaint with a supervisory authority;
i) whether the provision of personal data is a statutory or contractual requirement or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data.

Where personal data has not been obtained from the data subject, the Data Controller provides the data

subject with the above information and, in addition, in accordance with Article 14 of the GDPR, the following information:
a) the categories of personal data concerned;
b) the recipients or categories of recipients of the personal data, if any;
c) from which source the personal data originates, and where applicable, whether it came from publicly accessible sources.

Where personal data has not been obtained from the data subject, the Data Controller provides the information:
a) within a reasonable period after obtaining the personal data, but at the latest within one month;
b) if the personal data is to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or
c) if a disclosure to another recipient is envisaged, at the latest when the personal data is first disclosed.

The above information obligation need not be fulfilled if:
- the data subject already has the information contained in these points,
- the provision of such information proves impossible or would involve a disproportionate effort,
- obtaining or disclosure is expressly laid down by Union or Hungarian law applicable to the Data Controller which provides for appropriate measures to protect the data subject's legitimate interests, or
- where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Hungarian law.

The data subject's right of access - in accordance with Article 15 of the GDPR - extends to the provision of the following information:
- purposes of data processing;
- categories of personal data concerned;
- recipients to whom the personal data have been or will be disclosed;
- envisaged period for which the personal data will be stored;
- data subject's rights regarding the processing of personal data;
- source of the data, where they were not collected from the data subject;
- information about automated decision-making.

5. Rectification

The Data Controller rectifies inaccurate data without undue delay - if the necessary data and public documents proving them are available - and simultaneously informs the data subject in writing of the fact and time of the rectification.

For the period during which the Data Controller verifies the accuracy of personal data, the personal data in question is restricted in accordance with point 17.8 of this Notice.

If the data subject requests the rectification of their personal data and the personal data to which the already processed data should be rectified is not available, the Data Controller calls on the data subject to provide the missing information.

The Data Controller informs every recipient to whom the personal data has been disclosed of the rectification, unless this proves impossible or involves disproportionate effort. Upon request, the Data

Controller informs the data subject about these recipients.

6. Erasure

The Data Controller erases personal data without undue delay at the data subject's request if the data processing was based on consent, the data subject requests the erasure of the data (withdraws consent) and there is no other legal basis for data processing.

The Data Controller also erases personal data if:
- the personal data is no longer necessary;
- the data subject objects to the processing of their personal data in accordance with Article 21 of the GDPR;
- the processing of personal data is unlawful;
- erasure of data is necessary to comply with a legal obligation.

The data subject's right to erasure may only be restricted in the exceptions set out in the GDPR, i.e., if any of the above grounds exist, the continued retention of personal data shall be considered lawful,
a) for exercising the right of freedom of expression and information, or
b) for compliance with a legal obligation (i.e., during the period corresponding to the purpose of data processing for activities recorded with legal obligation as the legal basis in the Data Processing Register), or
c) for archiving purposes in the public interest, or
d) for scientific and historical research purposes or statistical purposes, or
e) for the establishment, exercise or defence of legal claims.

The Data Controller erases personal data in such a way that it can no longer be restored.

The Data Controller informs every recipient to whom the personal data has been disclosed of the erasure, unless this proves impossible or involves disproportionate effort. Upon request, the Data Controller informs the data subject about these recipients.

7. Restriction of processing

The data subject may request the Data Controller to mark personal data stored about them for the purpose of limiting their future processing.

Processing may be restricted if:
- the data subject contests the accuracy of the data, the Data Controller restricts the processing of personal data for the period necessary to verify the accuracy of the data;
- the processing is unlawful and the data subject opposes erasure and requests restriction of use instead;
- the data controller no longer needs the data but the data subject requires them for legal claims;
- the data subject objects to the processing of personal data under Article 21 of the GDPR, pending verification of the objection.

For the duration of the evaluation of the data subject's objection to the processing of their personal data - but for a maximum of 5 days - the Data Controller suspends data processing, examines the grounds of the objection and makes a decision, about which it informs the applicant.

If the Data Controller restricts the processing of personal data, such personal data may only be processed during the restriction period - with the exception of storage - with the data subject's consent or for the establishment, exercise or defense of legal claims, for the protection of the rights of another natural or legal person, or for reasons of important public interest of the Union or a Member State.

If the Data Controller lifts the restriction on processing, before lifting the restriction, it informs in writing the data subject at whose request the restriction was made, unless this proves impossible or involves disproportionate effort.

The Data Controller informs every recipient to whom the personal data has been disclosed about the restriction of processing, unless this proves impossible or involves disproportionate effort. Upon request, the Data Controller informs the data subject about these recipients.

If the restriction of processing was requested by the data subject, the Data Controller informs the data subject in advance about the lifting of the restriction.

8. Objection

The data subject has the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her based on the performance of a task carried out in the public interest or on legitimate interests. This means that the data subject may object to the processing of their personal data if the legal basis for data processing is:
- public interest under Article 6(1)(e) of the GDPR, or
- legitimate interest under Article 6(1)(f) of the GDPR.

When exercising the right to object, the Data Controller may no longer process the personal data unless the Data Controller demonstrates that the processing is justified by compelling legitimate grounds which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defense of legal claims. The Data Controller's managing director decides on determining whether compelling legitimate grounds justify the data processing. They inform the data subject of their position on this matter in an opinion.

For the period until the determination is made, personal data is restricted in accordance with point 17.8.

9. Data portability

The data subject has the right to receive the personal data concerning him or her, which he or she has provided to the Data Controller, in a structured, commonly used and machine-readable format and has the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:
- the legal basis for data processing is the data subject's consent or the processing was necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract [Article 6(1)(a) or (b) or Article 9(2)(a) of the GDPR] and
- the processing is carried out by automated means.

The data subject may also request the Data Controller to transmit personal data processed by it to

another data controller clearly designated by the data subject.

The right referred to in this point does not apply to the data subject if the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller, and if this right adversely affects the rights and freedoms of others.

10. Right to withdraw consent

If the legal basis for the Data Controller's processing of the data subject's personal data is the data subject's consent, then the data subject may withdraw their consent to data processing at any time. The data subject must be informed of this right and the method of withdrawal in the consent statement or in the data processing information provided at the same time. Withdrawing consent must be as easy as giving consent. The Data Controller may continue to process the data subject's personal data after withdrawal of consent given by the data subject for the purpose of fulfilling its legal obligations or enforcing its legitimate interests, if the enforcement of the interest is proportionate to the restriction of the right to protection of personal data.

11. Exercise of data subject rights after the data subject's death

Within five years after the data subject's death, the rights to which the deceased was entitled during their lifetime may be exercised by the data subject's close relative, or by a person authorized by the data subject through a disposition or by a statement made to the data controller in a public document or a private document with full probative force - if the data subject has made several statements to one data controller, by the statement made at a later date.

Liability, legal remedies, enforcement

The Data Controller is liable for the lawfulness of the processing of data subjects' personal data.

The Data Controller, as a data processor, is only liable to data subjects for damage caused by data processing if it has not complied with the obligations specifically imposed on data processors in the contract concluded with the data controller or in applicable legislation, or if it has disregarded or acted contrary to the lawful instructions of the data controller, otherwise the data processor is liable for the data processing activities carried out by the Data Controller as if it had acted itself.

A data subject who has suffered material or non-material damage as a result of an infringement of the GDPR is entitled to compensation for the damage suffered from the controller or processor.

In order to exercise their right to judicial remedy, the data subject may apply to court against the Data Controller or - in connection with data processing operations within the scope of the data processor's activities - the data processor if they believe that the Data Controller or the data processor commissioned by it or acting on its instructions processes their personal data in breach of the provisions on the processing of personal data laid down in legislation or in a binding legal act of the European Union.

All data controllers involved in the processing are liable for any damage caused by processing that infringes the GDPR. A processor is liable for damage caused by processing only where it has not complied with obligations of the GDPR specifically directed to processors or where it has acted outside or contrary

to lawful instructions of the controller.

If the Data Controller infringes the data subject's personality rights by unlawfully processing the data subject's data or by breaching data security requirements, the data subject may claim compensation for damages.

The Data Controller is liable to the data subject for damage caused by the data processor it uses and the Data Controller is obliged to pay the data subject compensation for personality rights infringement caused by the data processor. The Data Controller is exempted from liability for damage caused and the obligation to pay compensation if it proves that the damage or infringement of the data subject's personality rights was caused by an unavoidable cause outside the scope of data processing.

The Data Controller or processor is exempted from liability if it proves that it is not in any way responsible for the event giving rise to the damage.

If the data subject considers that the data processing violates the provisions of the GDPR or the Info Act, or finds the way the Data Controller processes personal data objectionable, they may file a complaint with the Data Controller at the contact details provided.

The data subject is entitled to file a complaint about the Data Controller's data processing procedure directly with the authority, they may file a notification with the National Authority for Data Protection and Freedom of Information (address: 1055 Budapest, Falk Miksa utca 9-11., postal address: 1363 Budapest, Pf. 9., telephone: +36 (1) 391-1400, E-mail: ugyfelszolgalat@naih.hu, website: www.naih.hu).

The data subject has the opportunity to go to court to protect their data, which will handle the case as a priority. In this case, they can freely decide whether to file their lawsuit at the court of their place of residence (permanent address) or their place of stay (temporary address) (http://birosag.hu/torvenyszekek). They can find the court of their place of residence or stay at http://birosag.hu/ugyfelkapcsolati-portal/birosag-kereso.

PART II: DATA PROCESSING AT THE DATA CONTROLLER

Data processing at the Data Controller

1. Contact

The Data Controller provides the opportunity for visitors to its Website (https://eccons.tech/) to contact the Data Controller using one of its contact details.

Purpose of data processing: Ensuring contact with the Data Controller.
Scope of processed data: The data subject's name, email address, content of the sent message.
Scope of data subjects: Persons establishing contact with the Data Controller.
Legal basis for data processing: The explicit consent of the data subject pursuant to Article 6(1)(a) of the GDPR.
Data storage period: Until withdrawal of consent and until the request is investigated and answered.
Method of data processing: Electronically
Source of data: Data collected from the data subject.

Possible consequences of failure to provide data: If the data subject does not make the data available to the Data Controller, they cannot contact the Data Controller. Failure to provide data does not result in adverse legal consequences for the data subject.
Automated decision-making and profiling: The Data Controller does not use automated decision-making and does not perform profiling.
Who can access the personal data?: The Data Controller's competent employees and employees of any data processors. The current list of the Data Controller's data processors is contained in this Privacy Notice.
Data transfer: No data transfer to third countries or international organizations takes place.

2. Processing of contact person data

The Data Controller maintains a register of its contractual partners. Regarding the maintenance of the register, it is important to point out that the Data Controller can, as a general rule, process personal data contained in contracts concluded with its partners only until the performance of the contract, based on the legal basis referred to in Article 6(1)(b) of the GDPR.

The Data Controller's contractual partners and contracted clients also include legal persons, whose data, as a general rule, do not qualify as personal data, and the Data Controller stores them for the purpose of contract performance. However, the data of individual contact persons specified in the contract, as well as possibly the data of contact persons of various authorities, who are not in a contractual relationship with the Data Controller but are merely employees, workers, or subcontractors of the Data Controller's contracted partners, fall under a different assessment. The Data Controller stores and registers the contact details and data of these persons to facilitate the Data Controller's activities and business operations, based on the Data Controller's legitimate interest.
The legitimate interest assessment test for maintaining contact person data is contained in the annex to this Privacy Notice.

Purpose of data processing: The purpose of data processing is to maintain a register of the Data Controller's contracting partners and their contact persons, and to maintain a register of authority contact persons.
Scope of processed data: The contracting partner's name, registered office, tax number, registration number, email address, telephone number, contact person's details (name, email, telephone number).
Scope of data subjects: The Data Controller's contractual partners, contact persons.
Legal basis for data processing: For the contracting party, based on Article 6(1)(b) of the GDPR for concluding and performing the contract, for the contracting party's contact persons based on Article 6(1)(f) of the GDPR, the Data Controller's legitimate interest.
Data storage period: For 5 years following the performance of the contract.
Method of data processing: On paper and/or electronically
Source of data: Data collected from the data subject
Possible consequences of failure to provide data: The provision of personal data is necessary for contract performance, if the data subject does not make the data available to the Data Controller, the Data Controller cannot perform the contract or maintain contact with the contractual partner.
Automated decision-making and profiling: The Data Controller does not use automated decision-making and does not perform profiling.
Who can access the personal data?: The Data Controller and its competent employees.
Data transfer to third countries or international organizations: No data transfer to third countries or

international organizations takes place.

3. Data processing related to maintaining records of the exercise of data subject rights under the GDPR

Purpose of data processing: Data processing related to maintaining records of the exercise of data subject rights defined in the GDPR.
Scope of processed data: The applicant's name, place and date of birth, mother's name, residential address, correspondence address, request for exercising data subject rights under the GDPR
Scope of data subjects: Person exercising data subject rights under the GDPR.
Legal basis for data processing: The legal basis for data processing is fulfillment of a legal obligation under Article 6(1)(c) of the GDPR and legitimate interest under point (f).
Data storage period: 5 years from the assessment of the request
Method of data processing: On paper and/or electronically
Source of data: Data collected from the data subject
Possible consequences of failure to provide data: It is necessary to process the data so that the Data Controller can comply with the provisions of the GDPR.
Automated decision-making and profiling: The Data Controller does not use automated decision-making and does not perform profiling.
Who can access the personal data?: The Data Controller, the Data Controller's competent employee.
Data transfer to third countries or international organizations: No data transfer to third countries or international organizations takes place.

4. Data processors

Data processors do not make independent decisions, they are only entitled to act in accordance with the contract concluded with the Data Controller and the instructions received. Data processors record, process, or handle personal data forwarded to them by the Data Controller and processed by them in accordance with the provisions prescribed by the GDPR. Data processors perform data processing operations on personal data provided by data subjects within the usage time available for each data processing purpose specified in this Privacy Notice. The Data Controller uses the following data processors in connection with the data processing described in this Privacy Notice. The current list of data processors is always available at the Data Controller.

Data processor category | Purpose of data processing | Data processor
Name | Registered office | Company registration number / registration number

Hosting provider | Hosting service | ININET Ltd. | 1063 Budapest, Szinyei Merse utca 10. | 01 09 970252
System administrator | System administration service | HardIT Solutions Ltd. | 2363 Felsőpakony, Zrínyi Miklós utca 11. | 13 09 222014

III. ANNEXES

Annex 1 - Notice to be included in contracts

The Client/Principal acknowledges by signing this contract that the Contractor/Agent will process the Client's/Principal's personal data provided during the conclusion of the contract and during the performance of the contract for 5 years from the termination of the contract, based on Article 6(1)(b) of

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter: "GDPR" or "Regulation"), in view of the contractual relationship established between it and the Client/Principal.

The Contractor/Agent maintains any contact person data contained in the contract based on its legitimate interest under Article 6(1)(f) of the GDPR. The Contractor's/Agent's legitimate interest assessment test is contained in the Privacy Notice.

Or

The Parties agree that during the conclusion and performance of this Contract, personal data of their natural person (company) representatives, employees and contributors (hereinafter collectively: "Contributor") will be disclosed in connection with this Contract as specified in the Contact point. Each Party is the data controller for its own Contributor, and the other Party is the recipient for the data controller Party's Contributor.

The Agent/Principal informs the Principal/Agent that the personal data of Contributors disclosed in connection with this Contract and coming to the Agent's/Principal's knowledge as a recipient will be processed by the Agent/Principal during the management and performance of the Contract for the purposes of document registration, invoice management, and organizational unit-level registration of business partner contacts, based on its legitimate interest under Article 6(1)(f) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter: "GDPR" or "Regulation").

The Principal/Agent informs the Agent/Principal that the personal data of Contributors disclosed in connection with this Contract and coming to the Principal's/Agent's knowledge as a recipient will be processed by the Principal during the management and performance of the Contract for the purposes of document registration, invoice management, and organizational unit-level registration of business partner contacts, based on the Principal's legitimate interest under Article 6(1)(f) of the GDPR.

Annex 2 - Legitimate interest assessment test for processing contact person data

Reason for conducting the legitimate interest assessment, purpose of data processing

The Data Controller maintains a register of its contractual partners. In connection with maintaining the register, it is important to point out that the Data Controller can, as a general rule, process personal data contained in contracts concluded during its activities only until the performance of the contract, based on the legal basis referred to in Article 6(1)(b) of the GDPR. However, the Data Controller has a legitimate interest in processing its clients' data listed in a register for the performance of the contract and for the possible enforcement of its legal claims.

Article 6(1)(f) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter: "GDPR") creates the legal basis for data processing if the processing is necessary for the purposes of the legitimate interests pursued by the

controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data.

Given that the data of individual contact persons is recorded by the Data Controller, and these persons are not directly in a contractual relationship with the Data Controller, the storage and registration of their data raises the limitation of the interests, fundamental rights and freedoms of the data subjects.

In order to determine whether the Data Controller's legitimate interest establishing data processing exists and thus whether data processing can be carried out for the purpose of registering contractual partners and their contact persons, it is necessary to conduct this legitimate interest assessment test.

During the legitimate interest assessment test, the following steps are taken and examined, taking into account the Article 29 Data Protection Working Party's opinion WP217, Annex 1:
- examination of the lawfulness of the data controller's interest;
- necessity test;
- fundamental rights or interests of data subjects;
- safeguards, and
- result of the legitimate interest assessment test.

The data controller's legitimate interest

The Data Controller may contract with natural persons, legal persons or organizations without legal personality acting within the scope of their profession, independent occupation or business activity. The data of legal persons and organizations without legal personality, as a general rule, do not qualify as personal data, the Data Controller stores them for the purpose of contract performance.

However, the data of individual contact persons specified in the contract, as well as possibly the data of contact persons of various authorities, who are not in a contractual relationship with the Data Controller but are merely employees, authorized representatives, beneficial owners, persons entitled to dispose or representatives of the Data Controller's contractual partners, fall under a different assessment. The Data Controller stores and registers the contact details (email, telephone number) and data (name) of these persons to facilitate the Data Controller's activities.

The purpose of data processing is in particular to achieve effective communication between the Data Controller and its contracting parties and partners, to conduct negotiations related to the contract, which forms an essential part of contract performance and is absolutely necessary for it.

The personal data that is the subject of this legitimate interest assessment test must necessarily be available during the term of the contract due to the need for orderly, single-channel management of contractual communication, which stems not only from the Data Controller's legitimate need but equally from that of its contractual partners and clients.

Necessity test

Why is the processing of personal data necessary to achieve the purpose?
The Data Controller has a fundamental and essential interest in maintaining contact with its contractual partner for the above-mentioned purpose. Processing personal data necessary for the creation,

performance, modification, and termination of the contract, without which the Data Controller cannot perform the contract or maintain contact with the contractual partner.

Is there an alternative solution available to achieve the purpose?
No alternative solution is available to replace the registration of personal data.

Can the data be processed on another legal basis?
The data subject's consent [Article 6(1)(a) of the GDPR] as a legal basis cannot be applied because the contact person is in an employment relationship with the Data Controller's partner, in which case the voluntariness of consent cannot be assumed due to the subordinate relationship.

Data processing cannot be based on contract performance either [Article 6(1)(b) of the GDPR] because no direct contractual relationship is established between the data subject and the Data Controller during the Service.

The Data Controller has examined the possibility of basing its data processing on the fulfillment of a legal obligation. Currently, there is no legal provision under which the Data Controller would be obliged to process the data of its contractual partners' contact persons.

Data processing cannot be based on the protection of vital interests of the data subject or another natural person [Article 6(1)(d) of the GDPR] based on available information.

The Data Controller is not a body performing public tasks or exercising public authority, so data processing based on Article 6(1)(e) of the GDPR would not be appropriate either.

What disadvantages would the Data Controller face if data processing does not take place?
If the data subject does not make the data available to the Data Controller, the Data Controller cannot perform the contract or maintain contact with the contractual partner. This prevents the smooth performance of the contract between the parties, so not only the Data Controller but also the contractual partner has an equal legitimate interest in processing the data.

The data subject's interests to be protected

The scope of persons affected by personal data processing includes the Data Controller's contractual partners, clients and persons designated as contact persons.

According to the Fundamental Law, everyone has the right to the protection of their personal data. The Fundamental Law further states that human dignity is inviolable. The data subject therefore has a protective interest in being able to exercise their right to informational self-determination; to control the processing of their personal data and to have their privacy respected by the data controller.

During the preparation of the legitimate interest assessment test, the Data Controller also took into account that data subjects can freely decide on their occupation, freely choose which employer they wish to contract with and with what content.

To protect the above, the Data Controller applies the safeguards and guarantees detailed in the following point.

Balancing of interests, safeguards

According to the above, the Data Controller's legitimate economic interests justify maintaining a register of its partners' contact person data and storing them, while the data subject's interest is that their personal data be processed appropriately, only to the necessary extent and bound to the purpose of data processing, until its realization.

The Data Controller keeps in mind that it only processes data necessary to achieve the purpose, thus paying attention to ensuring that the contact person's data is only processed and used to the extent necessary for concluding or performing the contract, and apart from this purpose, the data subject's private sphere and right to privacy are not violated.

The necessity of performing the contract between the data subject and the Data Controller's contractual partner as the data subject's employer also raises the existence of the employee's legitimate interest (which, however, does not necessarily coincide with the legitimate interest of the Data Controller and contractual partners). It follows from the employment relationship that the data subject maintains contact with their employer's contractual partners, so the data subject can also expect that the Data Controller will process their personal data used during their work performance in the above scope.

The Data Controller complies with the principles of the GDPR during its data processing, places special emphasis on appropriate and comprehensive information for data subjects, strives to maintain the highest level of data processing security and promote it. Data processing for data subjects is always carried out in a transparent manner. The Data Controller only processes data that is appropriate for the data processing purposes and absolutely necessary to achieve the given purpose.

To ensure the lawfulness of data processing, the Data Controller has carefully examined the legal bases for data processing, precisely specified the scope of data to be processed and their retention period, and ensured the exercise of data subjects' rights.

To ensure that the restriction is proportionate to the data subject's interests, the Data Controller applies the following safeguards:

The Data Controller has ensured that data subjects are appropriately, comprehensively and previously informed about the planned data processing and about the method of exercising their rights under the GDPR, their data subject rights and the Data Controller's contact details through the privacy notice related to data processing. The Data Controller also informs data subjects about the processing of contact person data in the contract concluded with the contracting partner.

The scope of processed data is limited to only the most necessary data, the processed personal data is necessary for achieving the data processing purposes as explained above. The Data Controller does not process data that is not relevant to achieving the data processing purposes. The processed personal data is as follows:
o The contractual partner's, client's name, telephone number, email address, contact person's details (name, email, telephone number).

The Data Controller processes the data for 5 years after the termination of the contract or until a new

contact person is reported, after which it immediately arranges for the deletion of personal data.

The processing of data subjects' personal data takes place exclusively for the purpose according to this legitimate interest assessment test, which purpose is specific, clear and lawful.

Secure storage of data is ensured, access to it is limited to the necessary extent and justified group of persons.

Data subjects are informed in detail about the method of exercising their rights under the GDPR, their data subject rights and the contact details of the Data Controller and its managing director through the privacy notice related to data processing, which is always available at the Data Controller's registered office.

Data subjects may at any time:
o exercise their right of access under Article 15 of the GDPR and request access to their personal data, as well as request data portability,
o exercise their right to rectification or erasure,
o exercise their right to restriction, and
o object to data processing by written request to the Data Controller's managing director

Data subjects may contact the Data Controller's managing director at any time with their questions regarding data processing or exercise their rights under the GDPR. Data subjects have been informed about the contact details of the Data Controller's managing director in the privacy notice related to data processing.

In view of the above, the processing of personal data by the Data Controller does not cause any disadvantage to the data subject.

Result of the legitimate interest assessment test

Based on the legitimate interest assessment test, it has been established that the enforcement of the Data Controller's legitimate interest is proportionate to the restriction of the data subject's interests with the introduction and compliance of appropriate safeguards, i.e., the use of the legal basis under Article 6(1)(f) of the GDPR can be considered well-founded.

In summary:
As a result of the legitimate interest assessment test, it can be established that the Data Controller's legitimate interest establishing the processing of data necessary for contract performance is stronger and more significant than the data subjects' interest in the Data Controller not knowing or processing this data. The lack of processing this data would in some cases make contract performance impossible, and thus the operation of the Data Controller.

The data processing purpose cannot be achieved by other means.

The rights and interests of data subjects are protected by numerous safeguards and guarantees built into the data processing process.

The data processing purpose is generally (by common understanding) accepted, and the data processing purpose cannot be achieved otherwise. The data subject is not disadvantaged by the data processing, moreover, they can only fulfill their contractual obligations arising from their legal relationship through data processing, i.e., it is also in the data subject's interest.