PRIVACY POLICY
eINGATLAN.hu

Effective from: June 01, 2024

Preamble

The Data Controller declares that it processes the data it manages in accordance with the applicable laws at all times, including the Fundamental Law of Hungary, Act CXII of 2011 on informational self-determination and freedom of information, and 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 ("GDPR").
The Data Controller respects the personal data of its employees, users, contractual partners, as well as visitors to the https://www.eingatlan.hu website. It treats all information and facts received confidentially and processes them solely based on the performance of contracts, legal requirements, and the prior consent of the data subjects.

Principles of Data Processing

The Data Controller conducts the processing of personal data in accordance with the following principles:
Data processing is carried out lawfully and fairly, and in a transparent manner to the data subject.
Data minimisation principle is applied, meaning that data processing should be adequate, relevant, and limited to what is necessary for the purposes of processing.
Data processing should be accurate and, where necessary, kept up to date. Reasonable steps are taken to ensure that inaccurate data is promptly erased or rectified.
Personal data is stored for a limited period, necessary for the purpose of processing.
Measures are taken to ensure the security of personal data against unauthorised or unlawful processing and against accidental loss, destruction, or damage.
Personal data is processed only for the purposes and in the manner specified in this Declaration, for the exercise of the rights and fulfilment of obligations defined herein. The Data Controller declares that it complies with these purposes at every stage of data processing.
The Data Controller only processes personal data that is essential for achieving the purpose of processing, in a manner suitable for achieving the purpose, and only to the extent and duration necessary to achieve the purpose.
Appropriate technical or organisational measures are implemented to ensure the proper security of personal data against unauthorised or unlawful processing, accidental loss, destruction, or damage.
The Data Controller declares that the principles of data protection do not apply to anonymous information, namely information that does not relate to an identified or identifiable natural person, and to personal data that has been anonymised in such a way that the data subject is no longer identifiable, for example, for statistical or research purposes.

Notification of Data Subjects

The Data Controller, by publishing this Declaration, takes appropriate measures to ensure that data subjects receive all information regarding the processing of personal data in a concise, transparent, understandable, and easily accessible form, clearly and comprehensibly formulated. Employees, partners, and Data Processors assisting the Data Controller are obligated to maintain confidentiality regarding the personal data of data subjects.

Interpretative provisions:
1. Data security: The combined system of technical, personal, and organisational measures and procedures taken to ensure the security criteria of data, such as confidentiality, integrity, and availability.

2. Data processing: Any operation or set of operations performed on personal data or sets of data, whether automated or non-automated, 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.

3. Data processing restriction: The marking of stored personal data with the aim of limiting their processing in the future.

4. Data Controller: Any natural or legal person, public authority, agency, or any other body which determines the purposes and means of processing personal data independently or jointly with others;

Data Controller according to this Declaration

The Data Controller:
Name: Info Sierra Kft.
Registered office: 1162 Budapest, Ferenc utca 2.
Company registration number: 01-09-886026
Tax identification number: 14038376-2-42
Website: https://www.eingatlan.hu
Email address: hello@eingatlan.hu

5. Data processing: Performing technical tasks related to data processing independently of the method and tool used for the execution of operations and the location of the application, provided that the technical task is performed on the data;

Data Processor: Any natural or legal person, public authority, agency, or any other body that processes personal data on behalf of the Data Controller under a mandate agreement concluded with them.

The data necessary for accounting purposes is always managed by employees or other legal persons who have obtained access rights from the Data Controller.

The Data Controller manages its IT infrastructure itself. The Data Controller stores personal data in its own server park located at the server hotel operated by Deninet Kft., at 18-22 Victor Hugo Street, Budapest XIII. The general terms and conditions of the server hotel are available at the following link: https://www.deninet.hu/aszf20220706.pdf, and the service quality indicators, annual reports, supervisory authorities can be found here: https://deninet.hu/ugyfeleinknek.
The Data Controller declares that data processors contracted with them only use personal data in accordance with the instructions of the Data Controller, for the intended purpose, and do not perform any other data processing operations. Data processing respects the personal data of data subjects and the provisions of this Privacy Statement.

6. Data destruction: The complete physical destruction of the data carrier containing the data;

7. Data erasure: Making the data unrecognisable in such a way that their restoration is no longer possible;

8. Data transmission: Making the data accessible to a specific third party;

9. Data locking: Marking the data with an identifier to restrict further processing for a permanent or specified period;

10. Data breach: A breach of security resulting in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access to personal data transmitted, stored, or otherwise processed;

11. Confidentiality: The characteristic of data that allows access only to a predefined user group (authorized users), with access by anyone else being illegal;

12. Loss of confidentiality: Loss of confidentiality is referred to as disclosure, where confidential data becomes known and/or accessible to unauthorised parties;

13. Security event: Any event that could have a detrimental effect on the confidentiality, integrity, or availability of information technology or data stored therein;

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

15. GDPR: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data;

16. Third party: Any natural or legal person, public authority, agency, or any other body other than the data subject, the Data Controller, the Data Processor, and the persons who, under the direct authority of the Data Controller or the Data Processor, are authorized to process personal data;

17. 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;

18. Info Act: Act CXII of 2011 on informational self-determination and freedom of information;

19. Integrity: The criterion of the existence, authenticity, integrity, and completeness of data, information, or program, ensuring that only authorized persons can modify them and they cannot be changed unnoticed;

20. 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;

21. Objection: A declaration by the data subject objecting to the processing of their personal data, requesting the cessation of processing or the deletion of the processed data.

Presentation of Data Controller's Activities, Liability Exclusion

The Data Controller is an economic company engaged in software development, whose main profile is to provide users with a digital platform capable of centralising real estate-related administrative tasks, in such a way that it can provide real estate portfolio management and handling through the so-called "eINGATLAN" application developed for this purpose.

As a developer and service provider company, the Data Controller is responsible for providing the platform, ensuring hosting, and for the operation of the software. The content is determined by the user themselves.

The Data Controller undertakes to ensure that the conclusion of license agreements is subject to compliance with the requirements of lawful exercise of rights, and to draw users' attention to compliance with personality rights and data protection regulations. At the same time, it excludes liability if the user uses the interface in a manner contrary to legal regulations. The Data Controller states that it does not regularly monitor the content uploaded by users; however, it expressly reserves the right to check and, if necessary, remove such content reported by others, which causes harm to others and violates legal regulations.

I process your personal data based on the following legal bases:
Data processing based on the performance of a contract [Article 6(1)(b) of the GDPR]
The performance of a contract includes agreements concluded between the Data Controller and its customers and other contractual partners.
Personal data of contractual partners:
Name/legal entity; address/registered office; contact person's name; phone number; email address
The purpose of processing the data is to conclude the relevant (usage, service, license) agreements, fulfill contracts, and provide contact details.
The Data Controller stores the provided personal data in digital form on a cloud-based digital server. Personal data is processed from the conclusion/establishment of the contract until the termination of the contractual relationship or the expiration of the limitation period for contractual claims. The processed personal data is not transferred to third parties.

To avail the services of the eINGATLAN subscription agreement, the customer needs to register. The required data for registration must be provided accurately and truthfully during the registration and data upload process.

Registration is carried out by the Data Controller (system administrators) for the customer simultaneously with the conclusion of the eINGATLAN subscription agreement, during which the following data is processed:
- Customer's last name
- Customer's first name
- Customer's email address
- Customer's billing information

After a valid registration, the customer becomes entitled to use the number of user accounts specified in the Subscription Agreement. Thus, the designated user(s) ("User") become(s) entitled to log into the Customer's account and use its functions. The user accounts have unique login credentials and are suitable for using modules and functions corresponding to the subscription. The customer can use eINGATLAN through their user accounts.

The Data Controller stores the provided personal data in digital form on a cloud-based digital server. The personal data provided to create the account is processed until the account is deleted. The Data Controller does not transfer the personal data processed in this context to third parties.

Data processing based on legal obligations [Article 6(1)(c) of the GDPR]
The following personal data of contractual partners is processed based on legal obligations regarding accounting, value-added tax, and tax regulations:
- Name/legal entity
- Address/registered office
- Tax identification number

The processing of contractual partners' data is done for the purpose of issuing invoices related to purchases and fulfillments.
The Data Controller stores the provided personal data in digital form on a cloud-based digital server and forwards it to the Data Processor responsible for accounting and payroll processing. Invoices are issued using an online invoicing program. The Data Controller manages the issued invoices, along with the data contained therein, until the statutory retention period for accounting purposes.

Data processing based on consent [Article 6(1)(a) of the GDPR]
The Data Controller allows individuals to request information about their products and services or seek telephone assistance related to their existing subscription through the https://www.eingatlan.hu website.

In this context, the Data Controller processes the following personal data of interested parties:
- Name
- Phone number

- Email address

The Data Controller stores the provided personal data in digital form on a cloud-based digital server. The personal data provided during the contact process is processed until the submission of the offer, but for a maximum of 1 year. The Data Controller does not transfer the personal data processed in this context to third parties.

Through the website https://www.eingatlan.hu, the Data Controller enables individuals to order the selected service directly from the Data Controller. Interested parties also have the option to request DEMO access directly via the email address hello@eingatlan.hu, where they can familiarize themselves with the operation and management of the eINGATLAN system.

In this context, the Data Controller processes the following personal data of interested/requesting parties:
- Name
- Email address
- Phone number
- Number of sub-accounts

The Data Controller stores the provided personal data in digital form on a cloud-based digital server. The personal data provided during the contact process is processed until the submission of the offer, but for a maximum of 1 year. The Data Controller does not transfer the personal data processed in this context to third parties.

Individuals have the opportunity to subscribe to informational letters (newsletter) from the Data Controller through the Data Controller's website.

In this context, the Data Controller processes the following personal data of the individuals:
- Name
- Email address

The Data Controller stores the provided personal data on the website's database interface and in digital form on a cloud-based digital server. The personal data of individuals are processed until the withdrawal of consent. The Data Controller does not transfer the personal data processed in this context to third parties.

Legitimate interest-based data processing [GDPR Article 6(1)(f)]

Individuals have the opportunity to grant usage rights to various people and organisations (e.g., legal representatives, accountants) for their own User Accounts and invite additional users.

In this context, the individual provides the Data Controller with the email addresses of the additional participants they wish to invite.

The Data Controller approves the access request for the provided email address and sends a joining link, clicking on which the invited participant can join the User Account. Refusal to provide the data constitutes an obstacle to concluding the contract. Providing and correctly stating the data is in the interest and responsibility of the user.

The purpose of data processing is to enable access to the User Account. The informational email sent by the Data Controller allows the possibility to object to personal data processing based on this legal basis. The Data Controller stores the provided personal data in digital form on a cloud-based digital server. The personal data provided in this way is processed until the withdrawal of access rights by the authorized user, but for a maximum of 1 year from the termination of the legal relationship, and until the expressed objection of the invited participant. The Data Controller does not transfer the personal data processed in this context to third parties.

The Data Controller informs data subjects in this Declaration that it lawfully processes such personal data that do not relate to identified or identifiable natural persons, as well as personal data that has been anonymised in such a way that the data subject is no longer or cannot be identified, for research or statistical purposes. In this regard, the Data Controller states that the statistical purpose includes the collection and processing of personal data for statistical surveys or calculation of statistical results.

The Data Controller declares that the further retention of personal data for such purposes can be considered lawful under the current data protection regulations. During such data processing, the Data Controller ensures appropriate guarantees regarding the rights and freedoms of data subjects. Based on its prior assessment, the Data Controller may proceed with the further processing of personal data for research or statistical purposes, as it exclusively uses data that does not or no longer allows the identification of data subjects.

Data Processing Activities:

The Data Controller provides data processing services to Clients who contract with it through the User Account. (Hereinafter within this section: "Data Processor"). The Data Processor, within the User Account, stores data uploaded by the representatives of Housing Cooperatives, performs operations related to them based on the explicit instructions of the Cooperative's representative, in accordance with the provisions of a separate contract concluded with the Cooperative. Upon the express separate request of the Cooperative's representative, the Data Processor carries out data upload to the User Account. Upon confirmation of the data upload and its correctness, the Data Processor does not perform any further data entry.

Typically, such data include the names of natural persons; birth name; place and date of birth; mother's name; address; email address; telephone number; name of the bank where the account is held; account number; tax identification number; personal identification number.

The Data Processor undertakes to carry out the processing of data entrusted by the Client as an data controller in compliance with this Declaration, and the requirements of data protection laws concerning it, ensuring compliance with the rights of data subjects and protecting their rights with appropriate technical and organisational measures.

The Data Processor undertakes to:

- Handle personal data only based on the written instructions of the data controller;
- Ensure that persons authorized to process personal data commit themselves to confidentiality;
- Take appropriate measures in the event of a personal data breach;
- Assist the data controller in fulfilling data subject rights by taking appropriate technical and organisational measures;
- Upon completion of the data processing service provision, delete or return all personal data to the data controller, and delete existing copies, unless EU or Member State law requires data storage;
- Provide the data controller with all information necessary for them to demonstrate compliance in case of a supervisory authority investigation;
- Before processing transmitted personal data, carry out necessary technical and organisational data security measures, considering the state of the art, costs of implementation, nature, scope, context, and purposes of processing, and varying likelihood and severity of risks to the rights and freedoms of natural persons, ensuring:
  (i) pseudonymization and encryption of personal data;
  (ii) ensuring the ongoing confidentiality, integrity, availability, and resilience of systems and services used for personal data processing;
  (iii) the ability to restore availability and access to personal data in a timely manner in the event of a physical or technical incident;
  (iv) a process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of processing;

(v) that persons acting under its authority who have access to personal data process them only in accordance with the instructions of the data controller, unless required to do so by EU or Member State law;
- Immediately inform the Data Controller of:
(i) any prohibition on disclosure, such as a legally binding prohibition on disclosure for the purpose of a criminal investigation by law enforcement authorities, in the absence of any contradictory prohibition;
(ii) any accidental or unauthorised access; and
(iii) any inquiries directly from data subjects, without responding to them, unless authorized to do so;
- Inform the data controller if it believes that any of its instructions violate the GDPR provisions.

The Data Processor keeps a record of all categories of data processing activities carried out on behalf of the data controller, including:

- The name and contact details of the data processor;
- The categories of processing activities carried out on behalf of each data controller;
- If applicable, transfers of personal data to third countries or international organisations;
- A general description of the technical and organisational security measures applied for data security.

The Data Processor may not engage another data processor without prior written authorisation from the data controller, whether in specific cases or general terms. In the case of general written authorisation, the Data Processor must inform the data controller of any circumstances that necessitate the involvement of additional data processors. The Data Processor must enter into a written agreement with any additional data processor it engages, which imposes the same obligations on the additional data processor as set forth in this declaration. If the additional processor fails to fulfil its data protection obligations arising from this written agreement, the Data Processor is fully responsible to the Data Controller for ensuring compliance with the obligations of the additional processor.

The Data Processor is only authorized and obligated to store data as long as the contract with the Housing Cooperative, as the Data Controller, or the Property Manager, regarding storage and processing, remains in force. In the event that the mandate of the Property Manager, who has contracted with the Data Processor, is terminated concerning the specific Housing Cooperative, the Data Processor must act based on a resolution of the general meeting containing revocation and new appointment. The Data Processor records that, after the termination of the contract, it stores the data only based on the express decision of the Data Controller; otherwise, the Data Processor creates a backup of the stored data in a format and transfers it to the rightful owner, which facilitates the restoration of data in the Data Processor's software system in case of a new contract with the Data Processor. Upon transferring the backup, the Data Processor permanently deletes the data from its own system. The continued storage of data as described above or returning it in the indicated format precludes the occurrence of a data protection incident.

During the execution of tasks by the data controller and the data processor, they are obliged to cooperate with the supervisory authority upon its request.

The Data Controller ensures that similar expectations are placed on data processors contracted by them as those complied with by the Data Controller's contracting parties during data processing operations in this chapter.

Access, Use, and Transmission of Data
Only the person who is obligated to do so for the enforcement of their obligations is entitled to access personal data stored about the data subjects. The Data Controller records the name of the person who handles personal data or is otherwise authorized to access it, the reason and time of access to the data in a protocol.

During data processing activities, there may be occasions where the processed personal data is used. Use is considered when personal data is used as evidence in court or other official proceedings. Anyone whose rights or legitimate interests are affected by the recording of personal data can request within 3 (three) working days from the recording of the personal data, with proof

of their rights or legitimate interests, that the Data Controller does not destroy or delete the data. If the Data Controller is requested by an authority or court to provide and release data, the Data Controller must provide the personal data if all conditions are met. If within 30 (thirty) days of the above request, there is no request for the omission of destruction by the Data Subject, the recorded image, and/or sound recordings, as well as other personal data, must be destroyed or deleted.

When transferring data to a third country or international organization, the Data Controller complies with the provisions of Chapter V of the GDPR to ensure that the level of protection guaranteed to natural persons is not compromised in any way.

Data Protection Incident
The Data Controller operates the hello@eingatlan.hu electronic contact for reporting any data protection breaches related to the data they or the Data Processor manage.

The Data Processor is obliged to report any possible data protection incidents to the Data Controller within 24 hours electronically after becoming aware of them.

The Data Processor must investigate and decide within 48 hours of receiving or becoming aware of a data protection breach reported or detected internally whether the potential breach poses a risk to the rights and freedoms of the data subjects.

If the investigation reveals that no data protection breach has occurred, the Data Controller informs the potential reporter and closes the case.

If it is confirmed after the investigation that a breach has occurred, the Data Controller:
a. Reports to the competent supervisory authority within 72 hours of becoming aware of the breach.
b. If the report cannot be made within 72 hours, the reason for the delay is indicated in the report, and the required information is provided in detail without further undue delay.
c. If it is confirmed after the investigation that a breach poses a high risk to the rights and freedoms of natural persons, the Data Controller informs the data subject about the data protection incident within 72 hours of becoming aware of it.

The Data Controller provides the data subject with clear and understandable information about the nature of the data protection breach and informs them of the content of the mandatory report to the supervisory authority and provides information on all steps the data subject can take to protect themselves from the consequences of the breach. The information provided to the data subject is transmitted in a separate message form (via email, or in the absence of this, by postal mail, or in the absence of this, by SMS).

Notification of the data subject about the data protection breach is not necessary if the Data Controller:
• Implements appropriate technical and organisational measures and applies these measures to the data affected by the data protection incident;
• After the data protection breach, takes further measures to ensure that the high risk to the rights and freedoms of the data subject is unlikely to materialise in the future;
• Notifying the data subject would require disproportionate effort. In such cases, the Data Controller informs the data subjects through publicly available information (by publishing a notice on our website) or takes similar measures to ensure effective notification of the data subjects.

Rights of Data Subjects and Their Enforcement
Data subjects receive information about the data concerning them, the scope, purpose, legal basis of data processing, their rights, and their enforcement possibilities from the issued Data Processing Information.

a) Right to Information Request - Data subjects are entitled to information about the ongoing data processing; the contact details of the data controller; the purpose and legal basis of data processing; the legitimate interest of the data controller; the recipients of data transmission; the fact of data transmission; the duration of personal data storage; their rights; the possibility of

withdrawing consent; the possibility of lodging a complaint; and to request information on whether the provision of personal data is based on law or contractual obligation or a precondition for entering into a contract, and whether the data subject is obliged to provide the personal data, as well as the possible consequences of failure to provide data. The Data Controller cannot refuse to fulfil the data subject's request for exercising their rights unless the data subject cannot be identified. Administrative fees based on reasonable charges may be charged for additional copies requested by the data subject.

b) Right of Access - The data subject is entitled to access the data stored about them during data processing and receive information about the purpose, legal basis, storage, and storage period of the processed data. The right to information extends to correcting, deleting, limiting processing, or informing about filing a complaint with the supervisory authority. We will not refuse to fulfil the request of the data subject exercising their rights unless it can be proven that the data subject cannot be identified. Administrative fees based on reasonable charges may be charged for additional copies requested by the data subject.

c) Right to Rectification - The data subject is entitled to request us to correct any inaccurate or incomplete data concerning them based on a supplementary statement.

d) Right to Erasure (Right to be Forgotten) - Upon request of the data subject, we will delete the data stored about them if one of the following reasons exists:
(i) the personal data is no longer necessary for the purposes for which it was collected or otherwise processed;
(ii) the data subject withdraws their consent on which the data processing is based, and there is no other legal basis for data processing;
(iii) the data subject objects to the data processing, and there are no overriding legitimate grounds for the processing;
(iv) the personal data has been unlawfully processed;
(v) deletion is required to fulfil a legal obligation under applicable law.

The personal data managed by the Data Controller must be deleted within a short period after the cessation of the legal basis for processing, including the withdrawal of consent in the case of processing based on consent.

e) Right to data lock ~ We lock the personal data if the data subject requests it or if, based on the available information, it can be assumed that deletion would violate the legitimate interests of the data subject. The locked personal data may only be processed for as long as the purpose of data processing that excluded the deletion of personal data persists.

f) Right to restriction ~ If inaccuracies, unlawfulness, unnecessary nature, or the data subject's objection to the processing of personal data arise, the data subject may request that we restrict the processing of these data.

g) Right to data portability ~ The data subject has the right to receive the data provided by them in a machine-readable (PDF, DOC, Excel, TXT) format in order to transfer it to another data controller.

h) Right to object ~ If the processing of personal data concerning the data subject is necessary for the legitimate interests of the Data Controller or a third party, or for direct marketing, public opinion research, or scientific research, or in other cases defined by law, the data subject may object to the processing of personal data for such purposes at any time.

The objection will be examined, a decision will be made on its merits, and the requester will be informed in writing of the decision within the shortest possible time, but no later than 15 days from the submission of the request.

Data security
The Data Controller protects data with appropriate measures against unauthorised access, alteration, transmission, disclosure, deletion, or destruction, as well as against accidental destruction and damage, and against becoming inaccessible due to changes in technology. The

Data Controller makes nightly backups of the eINGATLAN system, allowing for system restoration in the event of critical errors or data loss.

In this context, the Data Controller acts in compliance with the applicable guidelines on information security and requires the same from its Data Processors.

A data breach incident policy is developed for cases of personal data breaches, which specifies the possibility of reporting a data breach and the responsible persons for remedying the data breach, as well as the applicable deadlines.

Records are kept of realised data protection incidents.

In the event of a violation of the data subject's rights, the data subjects may lodge a complaint with the National Authority for Data Protection and Freedom of Information (address: 9-11 Falk Miksa St., Budapest 1055; phone: +36 (1) 391-1400, fax: +36 (1) 394-1410, email: ugyfelszolgalat@naih.hu), and they are also entitled to seek recourse to the court having jurisdiction over the decision.

The Data Controller is obliged to compensate for any damage caused to others by the unlawful processing of personal data or by the breach of the requirements of data security. If the Data Controller violates the data subject's personality rights by unlawfully processing their data or by breaching the requirements of data security, the data subject may claim damages.

Lawfully recorded personal data, information, negotiations taking place to avoid disputes or during disputes between the parties may be used.

Description and management of cookies
Viewing content accessible to anyone on https://www.eingatlan.hu is possible without providing personal data.

The websites and applications operated by the Data Controller use the following so-called "cookies":
- Necessary and functional cookies ~ which serve the basic operation and remembering user preferences.

The purpose of handling data stored in cookies is to enhance user experience and develop online services of the website/application. The cookies used on the website/application do not store personally identifiable information. During the visit to the website/application, the user can remove or disable cookies placed on their computer at any time, or their browser can warn them if the website/application intends to send a cookie.

We inform our users that we may occasionally collect information about them from third parties or publicly available sources such as business register sources.

We inform our users that the use of cookies operated by our website/application requires the prior, informed consent of the user under Section 155 (4) of Act C of 2003 on Electronic Communications ("Eht."). Therefore, upon the first visit to the website, a message will appear at the bottom of the screen stating that the website uses cookies, as well as a link leading to this information. The user can consent to the use of cookies by clicking the "Allow" button.

If the user does not wish to accept certain types of cookies, they can set their browser to prevent the placement of unique identifier cookies, or their browser can warn them if the website/application wants to send a cookie.

If you would like to learn more about these functions and refine your cookie settings, please consult the instructions or help screen of your internet browser, or you can enable and disable online behavioral advertising of individual providers using the following link: http://www.youronlinechoices.com/hu/ad-choices

Effective: June 01, 2024