PRIVACY NOTICE
FOR OUR CLIENTS AND OTHER INTERESTED PARTIES

Dear Clients, Prospective Clients, and Other Interested Parties!
Please read this Notice carefully!

In accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation—GDPR — on the protection of natural persons with regard to the processing of personal data and on the free movement of such data) and the provisions of Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information (Info tv),
we would like to inform you below
about our law firm's data processing principles, the rights and obligations of data controllers and data subjects, and the processes and safeguards related to data processing:

I./ THE DATA CONTROLLERS

DR. CSABA TÓTH LAW FIRM and DR. NORBERT REGŐS LAW FIRM are considered joint data controllers with respect to certain data processing operations for the purposes of using a unified IT-based case management system and conducting joint case management.
1. Details of the Data Controllers:
Data Controller 1 – Name: Dr. Csaba Tóth Law Firm
Szombathely Bar Association, / Bar Association ID number (kasz.sz): 36070370
Registered office and mailing address: 9700, Szombathely, Király u. 31. I/5.
Phone numbers: 06/94/313-798, 06/30/417-8939, 06/70/3237668
Email address: drtoth@trh.hu
Website: www.drtothcsaba.hu
Representative of the Data Controller at : Dr. Csaba Tóth, Attorney at Law
Name of the Data Controller 2: Dr. Norbert Regős Law Office
Szombathely Bar Association, / Bar Association ID number (kasz.sz): 36067691
Registered office and mailing address: 9700, Szombathely, Király u. 31. I/5.
Phone numbers: 06/94/313-798, 06/30/417-8939, 06/30/520-8043
Email address: drregos@trh.hu.
Representative of the Data Controller: Dr. Norbert Regős, attorney

2./ Purpose and scope of joint data processing:
In the course of legal practice, it is necessary to ensure appropriate substitution with general authority so that, in the event the attorney is unable to perform their duties, the client's interests are not harmed as a result of such inability. The Joint Data Controllers are each other's substitutes registered with the relevant bar association.
The Law Office of Dr. Csaba Tóth and the Law Office of Dr. Norbert Regős, in order to handle cases more effectively and ensure smoother representation in certain matters, and to ensure that professional considerations are addressed from multiple perspectives; in addition to providing for substitution, they organize their activities as a cost-sharing partnership to ensure coordinated representation for the benefit of their clients.
To ensure the optimal operation of the jointly maintained, unified case management and administration system, the firm has decided to utilize shared IT oversight, jointly employ administrative staff, and establish close cooperation with attorneys and trainee attorneys who coordinate back-office operations.
Joint data processing covers the entire set of client data managed within the joint case management system.
The duties and responsibilities of the joint data controllers are governed by the joint data controller agreement entered into between them.
The agreement on joint data processing entered into by the data controllers is established in accordance with Article 26 of the GDPR.
In accordance with their agreement, the joint data controllers operate a unified IT-based case management system under joint data controller responsibility.
With regard to jointly employed staff, the data controllers jointly process the personal data of data subjects in the areas of case management and document management in a uniform manner to achieve common business objectives, and jointly determine the purposes and means of data processing.
The data processing activities carried out by the data controllers consist, in particular, of the recording, storage, use, and deletion of personal data collected in accordance with data protection laws, chamber regulations, and office regulations, for the purposes of ensuring a uniform level of case management and decision-making preparation, in accordance with the data processing purposes set forth in this privacy notice.
With respect to any data that is not necessary for joint decision-making related to the use of the joint case management system, the individual Data Controllers are not considered joint data controllers.
During joint data processing, individual data controllers process data—for which the data controller that recorded the data independently determines the purposes and means of processing personal data—on behalf of the other data controller.
The joint data controllers may process and store the personal data of data subjects for the duration of the legal relationship serving as the legal basis for the data processing recorded in the administrative system, as well as for as long as a claim may be asserted in connection with that legal relationship; if such a legal relationship has been terminated, they may process and

store the data for as long as a claim may be asserted in connection with its termination, or for as long as the data subject has permitted such data processing (e.g., archiving) pursuant to the contract entered into for the specific matter.
Data subjects may exercise their rights under the General Data Protection Regulation with respect to and against any data controller.
However, the data subject is entitled to contact any of the data controllers; both data controllers must comply with the request; the practical administrative tasks related to fulfilling the request are primarily handled by the attorney handling the case.
Main cases of joint data processing:

- **Processing of client data in the shared case management system (retainer agreements, case records, correspondence, etc.) – joint data processing**
- **Website operation and communication – the website domain owner/contracting firm is the primary data controller; the other firm involved in the specific matter acts as a joint data controller in cases of joint case management**
- **Personal data of shared employee(s) – joint data processing**

Main cases of independent data processing:

- **Cases handled independently, not jointly, recorded only in the relevant office's case registry**
- **The firm's own billing and accounting data, if not processed in a shared system.**
- **In-house communications for marketing purposes, if any office sends out a separate newsletter or informational material.**

3./ Data Protection Officer:
Data controllers are not required to appoint a data protection officer.

II. / PRINCIPLES

The Data Controller
-processes personal data **only fairly and lawfully, and in a manner that is transparent to the Data Subject** in accordance with the provisions of the **GDPR** and **the Info Act** ,
-in processing the Data Subject's personal data, it adheres to **the principles of purpose limitation, data minimization, proportionality, accuracy, limited storage, and accountability**; its data processing is characterized by integrity and confidentiality,
-processes only personal data that **is essential for the successful performance of its activities in connection with its operations and the achievement of its objectives**; such processing is carried out exclusively **for lawful purposes**, within the scope of exercising rights and fulfilling obligations, in accordance with the requirements of **fairness and lawfulness**,
-processes personal data **to the extent and for the duration necessary to achieve the purpose**,
-ensures, during data processing**, the accuracy, completeness**, and—if necessary in light of the purpose of the data processing—the up-to-date nature **of the Data Subject's personal data**, as well as that the Data Subject can be identified only for as long as is necessary for the purpose of the data processing (principle of accuracy),
-ensures the appropriate security of personal data during data processing by applying appropriate technical or organizational measures—in particular, measures designed to protect against unauthorized or unlawful processing, accidental loss, destruction, or damage to the data**,**
- with regard to data transferred to data processors in connection with data processing and the data processing operations carried out**, complies with and ensures compliance by data processors with the provisions of the GDPR and other applicable laws,**
-requires its **employees and business partners** who come into contact with personal data to access, process, and handle such data solely in connection with their job duties or responsibilities and in accordance with their authorized access rights,
-takes appropriate measures to **ensure** that **unauthorized persons cannot access or obtain such data.**

III./ LEGALITY OF DATA PROCESSING

1./ Purpose of data processing:
In the course of their legal practice, attorneys necessarily process personal data in connection with maintaining contact with their clients, partners, and, in some cases, opposing parties, as well as in connection with handling cases pursuant to their mandates.
The general purpose of data processing is to perform legal services, represent clients' interests, comply with laws governing the practice of law and the exercise of the legal profession, and fulfill obligations.
In the course of their legal practice, Data Controllers process data fairly and lawfully, in accordance with the purpose of the data processing.

2./ Possible legal bases for lawful data processing—depending on the legal services provided:
- the data subject's voluntary consent—based on prior information (GDPR Article 6(1)(a)) or
- the fulfillment of an obligation arising from a contract to be concluded with the data subject as a contracting party—or from agreements related to such a contract or the attorney-client relationship (Article 6(1)(b) of the GDPR) or
- compliance with a legal obligation relating to the practice of law (, Article 6(1)(c) of the GDPR) or

- data processing is necessary to protect the vital interests of the data subject or another person (Article 6(1)(d) of the GDPR)
- 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 controller (GDPR Article 6(1)(e))
- the processing is necessary for the purposes of the legitimate interests pursued by the controller (or a third party) (Article 6(1)(f) of the GDPR).

The legal basis for each data processing activity varies depending on the type of case. Typically, the following legal bases apply:

- Performance of a contract: data processing necessary for the conclusion and performance of the attorney-client retainer agreement
- Compliance with a legal obligation: e.g., client identification, case record-keeping, anti-money laundering obligations, billing
- Legitimate interest: e.g., processing the data of opposing parties or other persons involved in proceedings in the client's interest
- Processing the contact information of contractual partners
- Consent: in cases of communication or data processing not directly related to a specific assignment or legal obligation (e.g., general inquiries submitted via the website)

In certain types of cases (including, but not limited to, criminal cases, cases involving health conditions, situations affecting or related to privacy rights, or labor, administrative, **and** civil cases)**, the processing of special categories of data (e.g., health data, data relating to criminal liability, data indicating trade union membership, etc.) may become necessary in connection with the practice of law, depending on the nature of the case. The processing of special categories of data is lawful primarily under Article 9(2)(a)–(d) of the GDPR and takes place within the framework of the legal provisions governing the legal profession**.

3./ Information regarding automated decision-making—including profiling:
The Data Controller does not use automated decision-making.

IF YOU HAVE ANY QUESTIONS REGARDING THE CONTENT OF OUR PRIVACY NOTICE, PLEASE CONTACT US USING THE CONTACT INFORMATION PROVIDED ABOVE!

IV./ THE DATA SUBJECT'S RIGHTS AND THE EXERCISE OF THESE RIGHTS

1./ Data subjects—that is, clients, opposing parties, contacts, and website visitors—have the following rights, depending on the relevant data processing activities:
Right to prior information and right of access; right to request information (GDPR Articles 13–14, 15–22, and 34)
The data subject may at any time request information regarding the processing of their personal data in writing (via email or by mail sent to our postal address) or verbally (by phone), including whether data processing is currently taking place, as well as their rights and safeguards—in particular, the identity of the data controller and data processor, the legal basis for data processing, its purpose, duration, location of data storage, and data security measures. Please note that if you contact us by phone—and your request regarding data processing warrants it (e.g., if you request the deletion of your data)—we must verify your identity to determine whether you are authorized to make the request before we can fulfill it. If identification is not possible, we can only provide general information regarding data processing. For this reason, we recommend that you submit your question or request in writing whenever possible.
Right to Rectification (Article 16 of the GDPR)
Right to erasure (GDPR Article 17)
Right to restriction of processing (GDPR Article 18)
Right to data portability (GDPR Article 20)
Right to object (GDPR Article 21)
The data subject may object to the processing of their personal data if

- the processing (transfer) of personal data is necessary solely to assert the rights or legitimate interests of the Data Controller or the recipient of the data, unless the processing is required by law;
- the use or transfer of the personal data is for the purposes of direct marketing, public opinion polling, or scientific research;
- the exercise of the right to object is otherwise permitted by law.

Right to Withdraw Consent

- In the case of data processing based on voluntary consent, the Data Subject may withdraw consent at any time, which does not affect the lawfulness of the data processing carried out on the basis of consent prior to the withdrawal.

2./ Submitting Requests, Complaints, and Comments
The Data Subject may primarily and directly contact the Data Controllers' representatives regarding requests, complaints, or comments concerning the Data Controller's conduct using the contact information provided in Section I. The Data Controllers shall always endeavor to review any request from the Data Subject in cooperation with the Data Subject within the shortest possible time and to find a solution to adequately address the request.

The Data Subject may exercise their rights regarding data processing by submitting a request to the Data Controller. The Data Controller will respond to any inquiry made through any of its contact channels without delay, but no later than 30 days.
If necessary, taking into account the complexity of the request and the number of requests—this deadline may be extended by 2 months.
The Data Controller shall notify the Data Subject of the extension of the deadline within 1 month of receiving the request, specifying the reasons for the delay.
This information is provided free of charge if the requester has not yet submitted a request for information to the Data Controller regarding the same activity or set of data in the same year.
If the Data Subject's request is unfounded—particularly due to its repetitive or excessive nature— constitutes an abuse, the Data Controller may, taking into account the administrative costs associated with providing the requested information or taking the requested action, charge a reasonable fee that reflects the hours of work and materials used; if this fee is not paid, the Data Controller may refuse to act on the request, and the Data Controller shall inform the Data Subject in advance of such costs fees in advance.
We document requests from Data Subjects and the related actions in accordance with the principle of accountability, as set forth in the relevant appendix, and retain them for 5 years, in line with the general statute of limitations for civil claims.
The data subject's other rights regarding complaints and remedies are set forth in Section VIII of this notice.

3./ The Data Controller's procedures regarding the Data Subject's exercise of their rights:
The Data Controller fulfills its obligations regarding the rectification, erasure, and restriction of data processing in accordance with the provisions of Article 19 of the GDPR.
The data controller erases personal data if its processing is unlawful, if the data subject lawfully requests it, if the purpose of the data processing has ceased to exist, or if the statutory retention period for the data has expired, or if a court or the data protection authority has ordered it.
The data controller shall notify the data subject of the rectification and erasure, as well as all those to whom the data was previously transferred for the purposes of data processing.
This notification may be omitted if, in light of the purpose of the data processing, it does not infringe upon the data subject's legitimate interests.
The data subject may request the rectification or erasure of their personal data by contacting the data controller using the contact information provided in this notice. The only obstacle to erasure may be a statutory requirement or restriction related to data processing.
In the event of unsolicited data disclosure, the Data Controller shall notify the data subject. The Data Controller shall delete the unsolicited data five business days after notifying the data subject, in the absence of the data subject's express consent to data processing.

In the event of an objection, the Data Controller—while simultaneously suspending data processing—will review the objection as soon as possible after the request is submitted and will inform the requester in writing of the outcome.
If the objection is justified, the Data Controller shall cease data processing—including further data collection and data transfer—and shall block the data, and shall notify all those to whom the personal data subject to the objection was previously transferred, and who are required to take action to enforce the right to object.
The data controller may not erase the data subject's data if the data processing is required by law. However, the data may not be transferred to the recipient if the data controller has agreed to the objection or if a court has determined that the objection is justified.

It may happen that the client provides us with the personal data of other individuals (e.g., opposing parties, witnesses, relatives). In such cases, the client is obligated to ensure that the data subject is informed, in accordance with the law, of the data transfer and the data processing described herein. In light of attorney-client privilege, in certain cases the attorney is not subject to a separate obligation to inform the data subject pursuant to Article 14(5) of the GDPR.

V. DATA TRANSFER, RECIPIENTS OF PERSONAL DATA

1. Data Transfer
The Data Controller shall transfer the personal data of Data Subjects to third parties—except in cases of mandatory data transfers required by law—only with the Data Subject's consent, and for the purpose of achieving the data processing objective, fulfilling the Data Controller's legal obligations, or in response to requests from authorized authorities. Before complying with any official data requests, the Data Controller will examine, with respect to each piece of data, whether a legal basis for the data transfer actually exists.
Data processed by the Data Controller may also be transferred to entities commissioned by the Data Controller to provide IT data storage, bookkeeping, accounting, and tax services, as well as legal services, and, if necessary, to bodies authorized by law to resolve legal disputes, or to ad hoc legal representatives, who—unless otherwise provided in this policy—may not use the data for any purpose other than the specified one and are bound by a duty of confidentiality.
If data processing is carried out by a third party on behalf of the Data Controller, the Data Controller may only engage data processors who, with respect to every participant in the sub-processor chain, provide adequate guarantees for the implementation of appropriate technical and organizational measures to ensure compliance with the requirements for data processing as defined by law and the protection of the rights of Data Subjects.

Beyond the disclosure of data, statements, and fulfillment of obligations to supervisory and other authorities as required by law, the Data Controller will not transfer personal data to third parties outside the categories of persons specified in this policy without first notifying the Data Subjects and, where necessary, obtaining their consent.
As a general rule, we do not transfer personal data to countries outside the European Economic Area (EEA). If such a transfer becomes necessary due to the use of certain IT service providers or other partners, we will carry it out only if the applicable safeguards (e.g., an adequacy decision under the GDPR, standard contractual clauses) are in place and—if required by law—only after the data subject has been expressly informed and has given their consent. Currently, the website's data is stored on servers located within the EEA (Hetzner Online GmbH, Germany). Before commencing the processing of IT data, the Data Controller verifies whether the applications installed in its IT system transfer data to servers operated outside the European Union; it excludes such applications from its operations prior to receiving the data.

2./ Recipients
Depending on the specific circumstances of each case, the personal data of data subjects may be disclosed to the following recipients:

- **The data controller's attorneys and their staff (attorney trainees, assistants, administrative staff)**
- **Lawyers with whom the data subject has an ongoing partnership and who have been approved by the data subject to handle the case (e.g., back-office staff, permanent substitutes)**
- **Authorities, courts, and other proceedings bodies before which the case is pending**
- **The opposing party and its legal representative, to the extent necessary for handling the case....**
- **Data processors (e.g., IT service providers, hosting providers, accountants) with whom the data controller(s) have entered into a contract**

We necessarily transfer the data subject's data to the relevant authorities or the opposing party in the course of professional measures required to handle the case—whether in out-of-court, litigation, or administrative proceedings—and thus these parties and their employees become recipients of the data.
When transferring data, the Attorney strictly complies with the laws and ethical standards governing the practice of law.

VI. DATA PROTECTION

The Data Controller and Joint Data Controllers shall take measures to protect the data they process independently or jointly in order to mitigate risks, in particular against unauthorized access, alteration, transfer, disclosure, disclosure, erasure, destruction, damage, and inaccessibility resulting from changes in the technology used.
During data processing, the Data Controllers shall maintain confidentiality, integrity, and availability in accordance with applicable legal provisions—in particular, based on the regulations governing the practice of law.
To ensure data security, the Data Controller takes the following measures in particular:
- when storing personal data electronically, it ensures that electronic data is password-protected, maintains uninterrupted digital operations, provides up-to-date virus protection, uses a firewall, performs regular backups, and regulates access permissions,
-ensures the physical protection of data storage media and hardware used for data processing,
-ensures the physical protection of personal data during paper-based processing to prevent unauthorized access; to this end, the law firm is protected by an alarm system equipped with a security lock and remote monitoring, and access to the locked office is possible only with the appropriate access code,
-ensures compliance with and enforcement of the rules governing data protection, data security, and attorney-client privilege in legal practice by all parties involved.
To ensure data security, the Data Controllers utilize IT monitoring and have entered into a data processing agreement with the IT service provider in accordance with applicable laws.

VII./ DATA PROTECTION INCIDENTS

A data breach is defined as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to, personal data that is transmitted, stored, or otherwise processed. (GDPR, Article 4)
Please note that if you become aware of a data breach or a risk thereof, you must immediately notify the Data Controller's attorney using one of the contact details provided in Section I!
The Data Controller shall notify the competent supervisory authority of the data breach without undue delay and, where feasible, no later than 72 hours after becoming aware of the data breach, unless the data breach is unlikely to pose a risk to the rights and freedoms of natural persons.
If the data breach is likely to pose a high risk to the rights and freedoms of natural persons, the Data Controller shall inform the Data Subject of the data protection measures without undue delay.
We investigate every data breach and take appropriate measures to prevent, to the extent possible, the risk of recurrence. We keep a record of data breaches and incorporate the lessons learned from them into the development of our data protection systems at the system level.

VIII. COMPLAINT HANDLING, JUDICIAL AND ADMINISTRATIVE REMEDIES

In the event of a perceived or actual infringement of their rights, Data Subjects should first contact the Data Controller! The Data Controller will conduct an investigation based on the Data Subject's complaint within 30 business days.
If necessary—taking into account the complexity of the complaint and the number of requests—this deadline may be extended by 2 months.
The Data Controller shall notify the Data Subject of the extension of the deadline within 1 month of receiving the request, specifying the reasons for the delay.

The Data Subject may bring a lawsuit against the Data Controller or—in connection with data processing operations falling within the scope of the Data Processor's activities— — against the Data Processor if, in the Data Subject's opinion, the Data Controller or the Data Processor acting on its behalf or under its instructions processes the Data Subject's personal data in violation of the provisions set forth in legislation or in a binding legal act of the European Union governing the processing of personal data.
The Data Subject may, at his or her discretion, also bring the action before the court having jurisdiction over his or her place of residence or place of stay. The proceedings are free of charge for the Data Subject.

The Data Subject may request that the Authority initiate an investigation to examine the lawfulness of the data controller's actions if the data controller restricts the Data Subject's ability to exercise their rights or rejects a request to exercise such rights; furthermore, the Data Subject may request that the Authority conduct an official proceeding if, in their opinion, the data controller, or the data processor commissioned by the data controller or acting on its instructions, has violated the provisions governing the processing of personal data as set forth in legislation or in a binding legal act of the European Union.
In the report, the data subject shall provide information supporting the fact that he or she has attempted to exercise his or her rights with the data controller.
The procedure is free of charge for the data subject.
The data protection authority:
Name: National Authority for Data Protection and Freedom of Information (NAIH)
Headquarters: 1055 Budapest, Falk Miksa Street 9–11,
Mailing address: 1374 Budapest, P.O. Box 603
Phone: +36 (1) 391-1400
Email: ugyfelszolgalat@naih.hu
Please check the Authority's website (URL: http://naih.hu) for any changes to these contact details

IX. APPLICABLE LAWS

The Data Controller processes the personal data it handles in accordance with the mandatory, applicable European and Hungarian laws and data processing principles, and ensures the safeguards that serve the security of data processing; these regulations include, in particular but not exclusively:
-General Data Protection Regulation (GDPR) 2016/679 of the European Parliament and of the Council (on the protection of natural persons with regard to the processing of personal data and on the free movement of such data)
- the Fundamental Law of Hungary
-Act XX of 1996 on Methods of Identification Replacing Personal Identification Numbers and the Use of Identification Codes
-Act C of 2000 on Accounting (Accounting Act)
-Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information (Info Act)
-Act V of 2013 on the Civil Code (Civil Code)
-Act LXXVIII of 2017 on the Practice of Law (Law on the Practice of Law)
-Act LIII of 2017 on the Prevention and Combating of Money Laundering and Terrorist Financing (Pmt.)

X. DEFINITIONS

The most fundamental definitions of data protection and other provisions—primarily the GDPR, the Act on the Practice of Law, and other legislation—referred to in this Information Notice are as follows:

Client: A person (natural or legal person) in a client-attorney relationship with the attorney
Opposing Party: A person who, in the course of the attorney's professional activities, acts against the client, or who has interests that are presumed or actually contrary to the client's interests, or who asserts or intends to assert such interests, and whose personal data comes into the attorney's possession during the performance of legal services.
Data processing: any operation or set of operations performed on personal data, regardless of the procedure used, including, in particular, the collection, recording, organization, storage, alteration, use, retrieval, transmission, disclosure, alignment or combination, blocking, erasure, and destruction, as well as preventing further use of the data, taking photographs, audio or video recordings, and recording physical characteristics suitable for identifying a person (e.g., fingerprints or palm prints, DNA samples, iris scans).
Data Controller: a natural or legal person, or an organization without legal personality, who or which—within the framework established by law or by a binding legal act of the European Union—determines, either independently or jointly with others, the purpose of data processing, makes and implements decisions regarding data processing (including the means used), or has them implemented by a data processor. AGS qualifies as a Data Controller with respect to the personal data it processes in accordance with this policy.

Joint Data Controller: If one or more data controllers jointly determine the purposes and means of data processing, they are considered joint data controllers who, in accordance with data protection provisions, transparently define in an agreement between them the manner in which they will fulfill their obligations under the law, in particular the allocation of responsibility for their respective duties related to the exercise of data subjects' rights, unless otherwise specified by Union or Member State law. The AGS Group is considered a joint controller with respect to personal data processed by it under this policy within the joint case management, corporate governance, and document management system.
Data Processing: the totality of data processing operations carried out by a data processor acting on behalf of or pursuant to the instructions of the Data Controller.
Data Processor: a natural or legal person, or an organization without legal personality, that processes personal data on behalf of or pursuant to the instructions of the Data Controller, within the framework and under the conditions set forth by law or by a binding legal act of the European Union. AGS may engage a data processor to process the personal data it handles.
Representative: a natural or legal person established or residing in the Union and designated in writing by the Data Controller or Data Processor pursuant to Article 27, who represents the Data Controller or Data Processor with respect to the obligations incumbent upon the Data Controller or Data Processor under the General Data Protection Regulation;
Recipient: A natural or legal person, or an organization without legal personality, regardless of whether it is a third party, to whom the data controller or data processor makes the personal data available.
Public authorities that may access personal data in the context of a specific investigation in accordance with Union or Member State law are not considered recipients; the processing of such data by these public authorities must comply with the applicable data protection rules in accordance with the purposes of the data processing;
Third Party: a natural or legal person, or an organization without legal personality, other than the Data Subject, the Data Controller, the Data Processor, or those persons who, under the direct authority of the Data Controller or Data Processor, carry out operations related to the processing of personal data.
Data Subject: **Any natural person** who is identified or identifiable based on any information; an identifiable natural person is a natural person 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. For the purposes of this policy, a Data Subject is an employee of the Data Controller.
Consent: a voluntary, unambiguous expression of the Data Subject's will, based on adequate information, by which the Data Subject indicates, through a statement or other conduct that unambiguously expresses his or her will, that he or she consents to the processing of personal data concerning him or her.
A legal declaration whose voluntary nature may be in doubt due to a relationship of subordination between the Data Controller and the Data Subject shall not be considered consent.
Personal data: any information relating to the Data Subject (an identified or identifiable natural person). (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.)
Personal data retains this status during data processing as long as the link to the Data Subject can be reestablished. The link to the Data Subject can be reestablished if the Data Controller possesses the technical capabilities necessary for such re-establishment.
Special categories of ***data :*** any data falling within the 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 intended to uniquely identify natural persons, health data, and personal data relating to a natural person's sex life or sexual orientation.
Data destruction: the complete physical destruction of the data storage medium containing the data.
Data transfer: making data available to a specific third party.
Data erasure: rendering data unrecognizable in such a way that it can no longer be recovered.
Restriction of data processing: blocking stored data by marking it to restrict its further processing
Pseudonymization: the processing of personal data in such a way that it is no longer possible to determine to which specific natural person the personal data relates without the use of additional information, provided that such additional information is stored separately and technical and organizational measures are in place to ensure that this personal data cannot be linked to identified or identifiable natural persons
Profiling: any automated processing of personal data intended to analyze or predict aspects of a data subject's personal characteristics, in particular those related to work performance, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.
Data filing system: a collection of personal data organized in any manner—whether centralized, decentralized, or structured according to functional or geographic criteria—that is accessible based on specific criteria.
Data breach: a breach of data security resulting in accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to, personal data that is transmitted, stored, or otherwise processed.
Cross-border processing of ***personal data:*** a) the processing of personal data within the Union carried out in connection with the activities of a controller or processor established in more than one Member State at its places of business in those Member States; or b) the processing of personal data within the Union in connection with the activities of a controller or processor at a single establishment, where such processing substantially affects or is likely to substantially affect data subjects in more than one Member State;

XI. REVIEW AND AVAILABILITY OF THE PRIVACY NOTICE
REVISION AND AVAILABILITY

We reserve the right to review and amend this notice as necessary, which may be warranted by changes in applicable laws or in our data processing activities and the technology used for them.
If the amendment affects your personal data processed on the basis of your voluntary consent, we will notify you immediately and suspend the further processing of your personal data until you provide your consent again.
The currently effective Privacy Policy is always available here, published publicly on the website, as well as in printed form at our office.

Dr. Csaba Tóth Law Office,
Dr. Norbert Regős Law Office
Data Controller, Joint Data Controllers

APPENDIX
Details of Certain Data Processing Activities

1. <u>Contacting and maintaining contact with our firm outside the scope of an attorney-client agreement</u>
You may contact our offices through any of our publicly available contact details and provide your contact information, which we will generally process with your consent until you retain our services.
You can contact us through any of the contact details listed on our website, as well as via the contact form provided for this purpose.

Scope of Processed Data	Purpose of data processing	Legal basis for data processing
Customer's name, address (mailing)	Establishing and maintaining contact for the purpose of exchanging information	Consent of the data subject pursuant to Article 6(1)(a) of the Regulation
Customer's email address	Establishing and maintaining contact for the purpose of exchanging information	Consent of the data subject pursuant to Article 6 (1) (a) of the Regulation
Customer's phone number,	Establishing and maintaining contact for the purpose of exchanging information	In accordance with Article 6 (1) (a) of the Regulation, the data subject's consent

We use the personal data you provide when contacting us solely for the purpose of communicating with you; we do not share this information with third parties.
Duration of data processing: We process the personal data you voluntarily provide for varying periods depending on the nature of the contact—until you withdraw your consent; if no contract is concluded, we process the data for no longer than two years from the date of provision.
We do not retain data provided on the website after the necessary information has been provided, unless a legally enforceable claim arises in connection with the ad hoc contact; in such cases, we may retain the data for up to 5 years for the purpose of verifying the claim.

2./ <u>Data processing carried out within the framework of and in connection with the attorney-client agreement</u>
2.1. Identification of the client and data processing carried out for the purpose of fulfilling the mandate
Pursuant to Sections 1, 2, 3, 9, and 27 of Act LXXVIII of 2017 on the Practice of Law (the "Act on the Practice of Law"), a lawyer necessarily processes personal data in the course of their legal practice.
In the course of their practice, attorneys are bound by a duty of confidentiality in accordance with the provisions of the Act on the Practice of Law.
The scope of the data processed may be determined by the laws applicable to the lawyer's practice (e.g., mandatory elements of a contract) or by requests from authorities in specific administrative or litigation proceedings.
Pursuant to Section 32(1) and (2) of the Act on the Practice of Law, with the exception of engagements for legal advice, prior to concluding the engagement agreement, the attorney-at-law shall verify the identity of the client, the legal advisor of the Bar Association, the person contracting with the employer, or the person acting on their behalf.
The attorney shall verify the identity of any natural person whom he or she does not know, or whose identity is in doubt, by inspecting a document suitable for identification.
In order to verify that the natural person's information matches the registered data and that the documents presented by the person are valid, the attorney may request data from the personal data and address registry, the driver's license registry, and the travel document registry. The attorney shall submit the data request if there are doubts regarding the validity or authenticity of the data or documents.

Scope of Processed Data	Purpose of data processing	Legal basis for data processing
Client's name and address	Conclusion of a retainer agreement	Pursuant to Article 6(1)(b) of the Regulation, performance of the attorney-client retainer agreement
	Billing	Pursuant to Article 6(1)(c) of the Regulation: Legal obligation applicable to the data controller Section 169 of the VAT Act, Sections 167 and 169 of the Accounting Act
Client phone number, name	maintaining contact	Pursuant to Article 6(1)(b) of the Regulation, the performance of the attorney-client engagement agreement
client data pursuant to Section 32(3) of the Act on the Practice of Law; in case of doubt,	Verification of data collected during client identification	Legal obligation applicable to the Data Controller pursuant to Article 6(1)(c) of the Regulation Section 32(2) and (3) of the Accounting Act

additional data necessary for the assignment, where the data subject is the client	representation in accordance with the client's interests, performance of the service	Pursuant to Article 6(1)(b) of the Regulation: performance of the attorney-client engagement agreement; the obligation to cooperate arising from the agreement

Duration of data processing: 8 years from the termination of the contract; in the event of a legal dispute, if later, 5 years following the resolution of the dispute.

2.2. Data processing for the purpose of maintaining case records

Pursuant to Section 53 of the Act on Attorneys, the attorney maintains records to ensure verifiability of compliance with the rules governing the practice of law and to protect clients' rights in the event of the termination of the attorney's license to practice law.

Scope of Processed Data	Purpose of data processing	Legal basis for data processing
Data pursuant to Section 53(2) of the Act on the Practice of Law	Compliance with the statutory obligation to maintain a case register	Article 6(1)(c) of the Regulation: Legal obligation applicable to the data controller Section 53(1) and (2) of the Act

Duration of data processing: 5 years following the termination of the mandate; in the case of the countersigning of a document, 10 years following the countersigning of the document; in cases involving the registration of a right pertaining to real property in an official registry, 10 years from the date of registration of the right.

2.3. Record-keeping for Cases Requiring Mandatory Legal Representation

Pursuant to Section 33(1) of the Attorneys Act, the attorney shall maintain a record of cases in which legal representation is mandatory.

Scope of Processed Data	Purpose of data processing	Legal basis for data processing
Data pursuant to Sections 32 and 33(2) of the Act on Attorneys	Compliance with the statutory obligation to maintain a case register	Article 6(1)(c) of the Regulation: Legal obligation applicable to the data controller Sections 32 and 33(1) and (2) of the Act on Lawyers

(Section 33(1) of the Act on Attorneys: In cases where legal representation is mandatory, an attorney shall maintain a record of natural persons identified by means of a document suitable for at least personal identification, as well as of legal entities and other organizations, in order to promote the security of legal transactions and to enforce the limitations on the practice of law.

(2) The registry maintained for identified natural persons shall contain the following data:

a) personal identification data,

b) address,

c) citizenship, statelessness, refugee, immigrant, settled resident, or EEA citizen status,

d) the type and number of the identification document used for identification,

e) the identifier of the response received in connection with the data request specified in Section 32(3),

f) the case identifier for cases in which the identification of a natural person is mandatory,

g) the data specified in the Act on the Prevention and Combating of Money Laundering and Terrorist Financing.

(3) If, based on the verification pursuant to Section 32(8), the attorney determines that the data specified in paragraph (2)(a) through (d) and (g) have changed, the attorney shall record the changed data, indicating the date of the verification, in such a way that the previously recorded data remain accessible.

(7) The attorney shall process the data specified in paragraphs (2) and (4) for the period specified in the Act on the Prevention and Combating of Money Laundering and Terrorist Financing.)

Duration of data processing: 8 years from the termination of the contract.

2.4. Processing of contact information for clients and contractual partners

In the course of the attorney's relationships with contractual partners and clients, the attorney processes the contact information of the partners' representatives and contacts. Due to the nature of the data, it may be necessary to process personal data (name, email address, phone number). The data controller reminds contractual partners and clients to inform the contact persons and representatives they have designated of the fact that their data is being processed.

Scope of Processed Data	Purpose of data processing	Legal basis for data processing
Name, contact information (phone number, email address), and position of the contact person or representative	Ensuring effective cooperation with contractual partners and clients; recording data necessary for business communication	Pursuant to Article 6(1)(f) of the Regulation, the Data Controller's legitimate interest in ensuring the continuity and smooth operation of its business relationships

Data processing continues until the termination of the contractual relationship or, in the case of ongoing cooperation, until June 30 of the calendar year following the end of such cooperation (document destruction date). If the data is included in the agency agreement, we will store the data—in accordance with the rules governing the agency agreement—for 8 years from the termination of the agreement.

2.5. Data Processing Related to the Counter-Signing of Documents Serving as the Basis for Entry in a Public Register

The attorney is required to identify their clients when countersigning a document serving as the basis for entry into a public registry. The method of identification and the scope of the data processed are defined in Section 32 of the Attorney Act.

Scope of Processed Data	Purpose of data processing	Legal basis for data processing
Client: Data specified in Section 32(3) of the Act on the Practice of Law	To verify the client's identity	Pursuant to Article 6(1)(c) of the Regulation: Legal obligation applicable to the data controller Section 32(7) of the Act on Lawyers

(Section 32(2) of the Act on the Legal Profession: A lawyer shall identify a natural person whom he or she does not know, or whose identity is in doubt, by examining a document suitable for identification.
(3) In order to verify that the natural person's data matches the registered data and that the documents presented by the person are valid, the attorney shall consult the personal data and address registry, the driver's license registry, the travel document registry, and the central immigration registry:
a) natural person identification data,
b) citizenship, statelessness, refugee status, immigrant status, settled resident status, or EEA citizen status,
c) address,
d) a photograph,
e) signature,
f) the information specified in Section 18(5) of Act LXVI of 1992 on the Registration of Citizens' Personal Data and Addresses,
g) data as specified in Section 24(1)(f) of Act XII of 1998 on Travel Abroad and the document's period of validity,
h) data as specified in Section 8(1)(b)(ba)-(bb) of Act LXXXIV of 1999 on the Road Traffic Registry,
i) Section 76(d) of Act I of 2007 on the Entry and Residence of Persons Enjoying the Right of Free Movement and Residence, Section 80(1)(b) and (c), as well as Section 95(1)(g) of Act II of 2007 on the Entry and Residence of Third-Country Nationals, Section 96(1)(g), and Section 100(1)(b) and (c).
(6) If a natural person acts as an authorized representative on behalf of a client, the attorney is not required to separately verify the client's identity, provided that the power of attorney containing the client's identifying information has been countersigned by the attorney, drawn up by a notary public, the principal's signature has been certified by a notary public, or the power of attorney has been certified or re-certified by the competent Hungarian diplomatic or consular authority at the place of signature, or it has been affixed with an Apostille certificate.
Section 32 (7) Prior to countersigning the document serving as the basis for entry into the public registry, the attorney shall—for the purpose of verifying identity and the validity of the document—identify the persons and organizations making the legal declaration, as well as the persons acting on their behalf, in accordance with paragraphs (2) through (4) and (6).
Section 53 of the Act on Lawyers (5) In the case of the countersigning of a document, the attorney shall retain the document countersigned by him or her, as well as other documents arising from the matter involving the countersigning of the document—unless a longer retention period is prescribed by law or the parties have agreed to a longer retention period—for a period of ten years from the date of countersigning.)

Duration of data processing: 10 years from the termination of the contract.

2.6. Client Due Diligence Pursuant to the Pmt.

Pursuant to Section 6(1) of the Pmt., the Attorney is required to conduct customer due diligence in the following cases:
a) upon establishing a business relationship;
b) upon the execution of a transaction order amounting to or exceeding four million five hundred thousand forints;
c) in the case of a merchant, when executing a transaction order in cash amounting to three million forints or more;
d) upon the execution of a transaction order exceeding three hundred thousand forints that qualifies as a funds transfer as defined in Article 3(9) of the Decree;
e) in the case of an organizer of bets that do not qualify as remote gambling, when paying out winnings of six hundred thousand forints or more for bets organized via non-telecommunications devices and systems that do not qualify as

remote gambling; in the case of bets not classified as remote gambling organized via telecommunications devices and systems, upon the payment of a player's balance of six hundred thousand forints or more;
f) if data, facts, or circumstances indicating money laundering or terrorist financing arise, provided that due diligence has not yet been conducted in accordance with points a) through e) or i);
g) if doubts arise regarding the authenticity or accuracy of previously recorded customer identification data;
h) if a change in customer identification data is recorded and, based on a risk-sensitive approach, it is necessary to repeat the customer due diligence;
i) in the case of a currency exchange transaction amounting to or exceeding three hundred thousand forints.

Scope of Processed Data	Purpose of data processing	Legal basis for data processing
Customer data as specified in Section 7(2) of the Pmt.	Conducting customer due diligence and complying with legal obligations	Article 6(1)(c) of the Regulation: Legal obligation applicable to the data controller: Sections 6 (1), 7(1), and 7(2) of the Pmt.

(Section 7(1) of the Pmt.: In the cases specified in Section 6(1)(a) and (e)-(h), the service provider is required to identify the customer, the customer's authorized representative, the person authorized to act on the customer's behalf, and the representative acting on behalf of the customer, and to verify their identity.
(2) During the identification process, the service provider is required to record the following information:
a) natural person
aa) first and last name,
ab) maiden name and surname,
ac) nationality,
ad) place and date of birth,
ae) his or her mother's maiden name,
af) his or her address, or, in the absence thereof, his or her place of residence,
ag) the type and number of his or her identification document;
b) for a legal entity or an organization without legal personality
ba) its name and abbreviated name,
bb) the address of its registered office or, in the case of a foreign-based enterprise—if it has one—the address of its Hungarian branch,
bc) its main activity,
bd) the names and positions of those authorized to represent it,
be) — if it has one — the details of its agent for service of process as specified in subparagraphs aa) and af) of paragraph a),
bf) in the case of a legal entity listed in the commercial register, its company registration number; in the case of other legal entities, the number of the decision regarding its establishment (registration, incorporation) or its registration number,
bg) its tax identification number.
(3) In order to verify identity, the service provider is required to request the presentation of the following documents or is authorized to retrieve data from an official registry:
a) natural person
aa) in the case of a Hungarian citizen, an official identification document suitable for verifying identity and an official document certifying their address, the latter if their place of residence or stay is located in Hungary,
ab) in the case of a foreign national, a travel document or identity card, provided that it authorizes residence in Hungary, a document certifying the right of residence or a document authorizing residence, and an official document certifying a Hungarian address, if their place of residence or place of stay is located in Hungary;
b) in the case of a legal entity or an organization without legal personality, the person authorized to act on its behalf or under its authority
in addition to presenting the document specified in point (a), a document—not older than thirty days—certifying that
ba) the company has been registered by the commercial court or has submitted an application for registration; in the case of a sole proprietor, the commencement of sole proprietorship activities has been reported or the sole proprietor has been registered,
bb) in the case of a domestic legal entity not covered by subparagraph ba) of paragraph b), if its formation requires registration with an administrative authority or a court, such registration has been completed,
bc) in the case of a foreign legal entity or an organization without legal personality, registration or enrollment in accordance with the laws of its home country has been completed;
c) the instrument of incorporation of the legal entity or organization without legal personality, prior to the submission of an application for registration with a court or administrative authority.
(3a) The verification of the data specified in subparagraphs (ab) through (ac) and (ae) of paragraph (2)(a) may be omitted if the document presented for the purpose of verifying identity does not contain such data.
(3b) In the case specified in paragraph (3a), the service provider is required to record the relevant information indicating that the data specified in subparagraphs (ab) through (ac) and (ae) of paragraph (2)(a) were recorded without verification.
(5) For the purpose of verifying identity, the service provider is required to verify the validity of the identity document presented pursuant to paragraph (3) and, in this context, is required to ascertain the authenticity of the document.

(6) During the identity verification process, the service provider is required to verify, in the case of an authorized representative, the validity of the power of attorney, the authorized party's right to dispose of the account, and the representative's authority to act on behalf of the authorized party.
Section 57(1) of the Pmt. The service provider shall, in the records it maintains, retain data that does not constitute personal data—including data obtained during electronic identification— as well as all other data generated in connection with the business relationship, in the records it maintains, for a period of eight years from the termination of the business relationship or the fulfillment of the transaction order.
(2) The service provider shall, in the records it maintains, retain the documents or copies thereof obtained in the course of fulfilling the obligations set forth in this Act and in legislation based on its authorization, including documents obtained during electronic identification, as well as documents and copies thereof evidencing the fulfillment of the reporting obligation and the provision of data pursuant to Section 42, documents evidencing the suspension of the transaction pursuant to Sections 34 and 35, or copies thereof, as well as all other documents arising in connection with the business relationship, or copies thereof, for a period of eight years from the termination of the business relationship or the fulfillment of the transaction order.)

Duration of data processing: 8 years from the termination of the contract.

2.7. Data of Other Data Subjects

Data subjects: other participants in the proceedings, opposing party, legal representative of the opposing party, third parties not participating in the proceedings (e.g., data of a client's family member)
If the personal data originates from the client, the client is obligated to declare that they are authorized to process the data and transfer it to the Attorney, and that they have an appropriate legal basis for the data transfer, and that they have fulfilled the obligation to provide information; the client hereby guarantees this. Pursuant to Article 14(5)(a) of the Regulation—in light of the client's fulfillment of the obligation to provide information—the Attorney shall not provide separate information to the data subject.
The Attorney is not subject to a duty to inform if the personal data being processed is subject to attorney-client privilege (GDPR Article 14(5)).

Scope of Processed Data	Purpose of data processing	Legal basis for data processing
Additional data necessary for the engagement, where the data subject is a third party	Representation in accordance with the client's interests; performance of the service	Pursuant to Article 6(1)(f) of the Regulation: The legitimate interest of the Data Controller and the client in successful cooperation regarding the mandate and the effective performance of legal services

(Section 46(5) of the Act on Attorneys: Unless the parties have agreed to a longer retention period, the attorney shall retain the electronic document for ten years from the date the copy was made.
(6) A lawyer shall retain a paper-based document that has been converted into electronic form and countersigned by the lawyer—unless the parties have agreed to a longer retention period—for five years from the date of conversion.
Section 53 (5) In the case of the countersigning of a document, the attorney shall retain the document countersigned by him or her, as well as other documents generated in connection with the countersigning of the document—unless a longer retention period is prescribed by law or the parties have agreed to a longer retention period—for ten years from the date of countersigning.)

Duration of Data Retention: Statutory obligations applicable to attorneys establish the duration of data retention for each type of case. Attorneys shall retain data exclusively for the period specified by law.

2.8. Lawyer's Escrow Register

The attorney maintains a record of attorney escrow accounts in accordance with Section 7.4 of Regulation No. 7/2018 (March 26) of the Hungarian Bar Association on attorney escrow management and escrow records.

Scope of Processed Data	Purpose of Data Processing	Legal basis for data processing
the subject matter of the escrow the type of escrow, the date of conclusion or amendment of the escrow agreement, the date of termination of the escrow agreement; if the escrow is held by a custodial organization, the name and registered office of the custodial organization; if the escrow is placed with a court, the fact and date thereof; data related to the fulfillment of the escrow; in the case of funds received from a third party for the	Compliance with the statutory obligation to maintain a deposit register	Legal obligation applicable to the Data Controller pursuant to Article 6(1)(c) of the Regulation, Section 158 of the Act on the Practice of the Legal Profession Section 7.4 of Regulation No. 7/2018 (March 26) of the Hungarian Bar Association on the Custody of Funds by Attorneys and the Maintenance of Custody Records

benefit of the client, the date of receipt, the amount of funds received, and the legal basis for receipt;		

Duration of data processing: 10 years from the termination of the escrow agreement, in accordance with the referenced MÜK regulation.

2.9. Data transfer to cooperating law firms, agents, and deputies

It is in the legitimate interest of the attorney and the client (including cases where the client is not the data subject, particularly in the case of clients that are legal entities or other organizations, or with respect to the data of persons other than the client) to engage the assistance of additional law firms specializing in the relevant field, individual attorneys, European Community lawyers, or other consultants. Clients will be informed about the identities and, if necessary, the professional qualifications of these additional law firms, individual attorneys, European Union lawyers, and consultants—taking into account the specific nature of the relationship—during the course of the engagement, and the Attorney will take the clients' requests into account to the greatest extent possible when selecting such individuals.
The scope of data processed during data transfer depends on the nature of the specific engagement.
The legal basis for the data transfer, pursuant to Article 6(1)(f) of the Regulation, is the legitimate interest of the Data Controller and the client in the successful fulfillment of the mandate and the involvement of necessary experts.

3./ <u>Data Processing Related to Data Subject Requests</u>
The Attorney is required to maintain records of data protection requests and of the data processed in connection with the exercise of data subjects' rights.

Scope of Processed Data	Purpose of data processing	Legal basis for data processing
Personal data related to data protection requests: in the case of natural persons, legal entities, or other organizations, the contact information of the designated contact persons necessary for communication (including, in particular: name, address, email address), the content of the request, as well as the steps taken in connection with the request and the documents prepared in connection with the request	Compliance with the legal obligation to maintain a record of requests, in accordance with the principle of accountability	Legal obligation applicable to the Data Controller pursuant to Article 6(1)(c) of the Regulation Enabling the exercise of data subjects' rights as set forth in Articles 15–22 of the Regulation, and documenting other actions taken in connection with the request

Duration of data processing: in the absence of different guidelines from the data protection authority, 5 years from the date of the request, given that it is realistic to expect that any data protection claims may be enforced before a data protection authority or court within this period (Civil Code, Section 6:22 (1)—unless otherwise provided by the Civil Code, claims become time-barred after 5 years)

4./ <u>Data Processing Related to Data Breaches</u>
The Attorney is required to maintain a record of data protection incidents. This record enables the data protection authority to verify compliance with the requirements of the Regulation.

Scope of Processed Data	Purpose of data processing	Legal basis for data processing
the facts related to the data breach, its effects, and the measures taken to remedy it	Compliance with the legal obligation to maintain a record of incidents in accordance with the principle of accountability	Article 6(1)(c) of the Regulation: Legal obligation of the data controller; Article 33(5) of the Regulation

Duration of data processing: in the absence of different guidelines from the data protection authority, 5 years from the date of becoming aware of the data protection incident, given that it is realistic to expect that any data protection claims may be enforced before the data protection authority or a court within this period (Civil Code, Section 6:22 (1)—unless otherwise provided by the Civil Code, claims become time-barred after 5 years)

<u>5</u>./ <u>Data Processing by the Website, Cookies</u>
Anyone may view the public content of our website—without providing personal data—and doing so does not require registration or logging in.
In connection with your visit to and use of the website, we process the data listed below for the purposes and for the duration specified in this notice, and we ensure that you can exercise your rights regarding data processing as follows:

5.1. Use of Cookies

A cookie is a piece of data that the website sends to the data subject's browser, causing the browser to store certain information so that the website can restore the original settings upon a subsequent visit. Accordingly, when you open and use our website, a cookie is a text file placed on the device (computer, smartphone) during your visit to our website, which typically contains information regarding the connection between the web server and your device or the operation of the website (for example, a so-called session ID, which is a unique string of letters, numbers, and other characters; the time you opened or visited the website, etc.), the contents of which the web server occasionally reads back from the file—while you are browsing our website or when you visit it again later.

When visiting the website, the Data Subject is informed about the cookies used on the site. The Data Subject uses the website with this information in mind.

The content of the cookie enables the website (server) to improve the user experience and provide the services offered on the website.

The cookies used are not capable of identifying the Data Subject. Refusing to consent to the use of cookies does not result in any disadvantage to the Data Subject.

The Data Subject can delete cookies from their own computer or block their use in their browser. These options vary by browser but are typically found under the "Settings" or "Privacy" menu. The Data Controller displays a "Cookie Notice" when the Data Subject accesses the website.

The cookies used on the website can be classified into the following categories:

- **Strictly necessary (functional) cookies**: ensure the website's operation (session ID, security settings). Their use is essential for using the website, so consent is not required for their use
- **Statistical cookies (Google Analytics)**: used to measure website traffic and visitor statistics
- **Marketing cookies (Facebook Pixel)**: These enable the display of personalized ads.

When you first visit the website, a pop-up window will ask for your consent to the use of statistical and marketing cookies. We consider the use of strictly necessary cookies to be essential for the website to function, so their use cannot be disabled while using the website."

Purpose of Data Processing

To identify and distinguish between users visiting our website, to identify users' current sessions, to store the data provided during those sessions, and to prevent data loss.

Scope of data processed

The cookies used on our website are so-called functional cookies that support the website's operation; they contain the time of the visit, the session ID, and other session-related information (numeric and character strings) that can be interpreted by the website's program code.

We do not share the information stored in functional cookies with third parties.

Duration of Data Processing

Some of the functional cookies used on our website expire as soon as you leave the website or close the page in your browser. Some other functional cookies have a longer lifespan (180 days); however, our website can only access the content of these cookies if you revisit our website from the same device and have not deleted these cookies in the meantime.

Exercising Your Rights Regarding Cookies

Most web browsers automatically allow the use of cookies. However, you can change this setting at any time, block cookies, or delete them. You can access, review, and view the contents of the cookies stored on your device at any time.

To manage, disable, or delete cookies, most popular web browsers typically provide an option under their settings—usually in a submenu labeled "Security," "Privacy," or "Data Protection"—under the heading "Cookies."

Please note that if you disable or do not accept the use of cookies, certain features of the website will function differently or may not be available to you.

For more information on managing cookies, please refer to the help section of the respective browser or click on the browser name in the following links: Internet Explorer, Chrome, Mozilla Firefox, Edge.

• Google Chrome: https://support.google.com/accounts/answer/61416?hl=hu
• Firefox: https://support.mozilla.org/hu/kb/sutik-engedelyezese-es-tiltasa-amit-weboldak-haszn
• Microsoft Internet Explorer 11: http://windows.microsoft.com/hu-hu/internet-explorer/delete-manage-cookies#ie=ie-11
• Microsoft Internet Explorer 10: http://windows.microsoft.com/hu-hu/internet-explorer/delete-manage-cookies#ie=ie-10-win-7
• Microsoft Edge: http://windows.microsoft.com/hu-hu/windows-10/edge-privacy-faq
• Safari: https://support.apple.com/hu-hu/HT201265

5.2. Google Analytics

We use the Google Analytics service to analyze and measure our website's visitor traffic, traffic data, and performance. The Google Analytics service collects information for statistical purposes regarding the use of the website; this information does not serve to directly identify visitors. However, technical data related to the device and browser (e.g., IP address, cookie ID) may be classified as personal data under applicable data protection regulations. In the Google Analytics settings—where possible—we use IP anonymization and configure the service to the extent necessary to comply with GDPR requirements. You can read more about Google Analytics' data processing by clicking here.

Purpose of Data Processing

To measure the website's performance and compile statistics on its use by distinguishing between visitors to the website and their sessions.

Scope of data processed

The Google Analytics service uses cookies to measure the website's performance and to compile statistics on its use; these cookies contain information that can be interpreted by the service (unique strings of characters consisting of letters, numbers, and other punctuation marks).

Duration of data processing

The cookies used by Google Analytics may have different validity periods. Some cookies expire when you close the page in your web browser, while others have a shorter validity period (1 minute) or a significantly longer one (e.g., 24 hours or 2 years). However, our website—and, through it, the Google Analytics service—can only access the content of these longer-term cookies if you revisit our website from the same device and have not deleted these cookies in the meantime.

Exercising Your Rights

If you do not want the Google Analytics service to collect data about your visit to our website, you can prevent this by installing and using the software provided for this purpose. You can read more about the browser add-on that disables Google Analytics data collection by clicking here, and you can download and install it from here.

You can also disable the cookies used by Google Analytics—along with all other cookies. You can access, view, and delete the cookies stored on your device at any time.

5.3. Facebook Pixel

The Facebook Pixel is a code that allows the website owner to display personalized offers and ads to website visitors on Facebook by using Facebook's marketing services. By using this remarketing tracking code, Facebook is able to effectively display ads targeted at interested users (the target audience) and also provide the website owner with statistical data about website visitors. The Facebook Pixel also uses cookies to function. The Facebook Pixel is used only with your prior consent, which you can provide or withdraw at any time via the cookie notification interface displayed on the website.

For more information about Facebook's data processing, cookie management, and the use of Facebook Pixel, please visit:
https://www.facebook.com/about/privacy
https://www.facebook.com/policies/cookies/

Purpose of Data Processing

To distinguish between visitors to the website and their sessions, and to display personalized offers and ads on their Facebook pages.

Scope of data processed

The cookies used by Facebook Pixel contain information that can be interpreted by the service (unique strings of characters consisting of letters, numbers, and other punctuation marks).

Duration of data processing

The cookies used by Facebook Pixel are generally valid for 90–120 minutes. Our website—and, through it, the Facebook service—can only access the contents of these cookies if you revisit our website from the same device and have not deleted these cookies in the meantime.

Exercising Your Rights

You can also disable the use of cookies used by Facebook Pixel—along with all other cookies. You can access, view, and delete the cookies stored on your device at any time.

5.4. Data Processing for the Website

The IT infrastructure supporting the operation of our website is provided by our contracted service provider. The data processed on the website is stored within the European Union by our contracted partner.

Name of the data processor:	Hetzner Online GmbH
Registered office of the data processor:	Industriestr. 25, 91710 Gunzenhausen, Germany
Phone number of the data processor:	+49 (0)9831 505-0
The data processor's email address:	info@hetzner.com