

PRIVACY NOTICE

1. Introduction

- 1.1.** We would like to inform our Clients and other persons (hereinafter referred to as "Data Subjects") concerned with the processing of their personal data by **Dr. Simon Emese Júlia Law Office** (hereinafter referred to as "the Data Controller") about the following.

1.2. The identity of the Data Controller:

Name:	Dr. Simon Emese Júlia Law Office
Bar registration number:	4986
Chamber identification number:	36068340
E-mail:	office@simonlegal.hu
Telephone:	+36 (1) 810 1100
Mailing address:	1053 Budapest, Kossuth Lajos utca 7-9

- 1.3.** This Privacy Notice applies only to the personal data of natural person Data Subjects, with the understanding that the data of legal entities or other entities are not considered personal data.

- 1.4.** For law firms, the **following legislation** contains important provisions on data processing:

- Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation; also known as GDPR)
(<http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32016R0679&from=EN>)
- Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information (hereinafter: Infotv.)
(<https://net.jogtar.hu/jogszabaly?docid=A1100112.TV>)
- Act LXXVIII of 2017 on the Activities of Lawyers (hereinafter: Lawyers Act)
(<https://net.jogtar.hu/jogszabaly?docid=A1700078.TV×hift=ffffff4&txtreferer=00000001.TXT>)
- Act No LIII of 2017 on the Prevention and Combating of Money Laundering and Terrorist Financing (hereinafter: Money Laundering Act)
(<https://net.jogtar.hu/jogszabaly?docid=A1700053.TV>)

- 1.5.** The Data Controller does not make decisions based on automated processing or perform profiling. The Data Controller does not transfer personal data to a Member State outside the EEA, except where the nature of the assignment requires such transfer. In such cases, the transfer will be subject to appropriate safeguards.

- 1.6.** In many cases, the processing carried out by the Data Controller is based on law. In such cases, the data subject is obliged to provide his or her personal data. For example, the conclusion of an engagement letter is subject to the provision by the client of certain personal data as defined in the Lawyers Act and the Money Laundering Act and to the retention of such data by the lawyer (see point 2.1.6 below). In other cases, the provision of personal data is voluntary, but is in any case necessary for the performance of the mandate. If the data subject fails to provide the personal data that the Data Controller considers necessary for the performance of the mandate, the Data Controller may not be able to perform the mandate and thus not be able to provide legal advice to the data subject.

- 1.7.** Where processing is based on consent, the data subject has the right to withdraw his or her consent at any time. However, this does not affect the lawfulness of the processing prior to the consent.

2. Characteristics of each processing operation

2.1. PROCESSING CARRIED OUT IN THE COURSE OF THE ACTIVITIES OF LAWYERS OR LEGAL ADVISERS

2.1.1. Those affected:

- natural person clients to whom the Data Controller provides legal advice or other legal services;
- other natural persons concerned in connection with the mandate given to the Data Controller (e.g. a party to a legal proceeding or dispute with the principal, natural persons included in the file of a public authority or litigation, persons heard as witnesses);
- natural person contact persons of the Data Controller's customers.

2.1.2. Purpose of processing: in the course of the performance of the lawyer's duties, the Data Controller processes the personal data of the persons concerned by the given mandate, as defined below, and other personal data relevant to the case, for the purposes of the performance of the case, the provision of legal advice, the exercise of the lawyer's duties, the countersigning of documents, the provision of legal representation in official proceedings and litigation (depending on the case), and for the purposes of the identification, registration and reporting obligations required by law. The Data Controller also processes certain personal data for the purposes of maintaining contact, internal case records, billing and the enforcement of claims arising in the course of the mandate.

2.1.3. Legal basis for processing: the legal basis for processing by the Data Controller varies. Legal basis may include:

- the performance of an engagement letter between the Data Controller and the data subject (e.g. the performance of a mandate for the preparation and countersigning of a real estate sale and purchase agreement);
- to comply with a legal obligation to which the Data Controller is subject (see the legal provisions referred to in point 2.1.6 below);
- the legitimate interest of the Data Controller (e.g. in cases not covered by the legal obligation to keep documents for the purpose of subsequent proof of performance, maintaining contact during the performance of the contract, consistency of case management, recovery of claims). Legitimate interests: unified case registration and management, the right to enforce the fee for the mandate and to ensure unhindered communication during the performance of the service;
- the legitimate interest of a third party (e.g. the legitimate interest of the person who instructs the Data Controller in relation to the enforcement of a claim of the instructing party, the processing of personal data of the debtor of the claim by the Data Controller, or the processing of personal data of a party to a lawsuit against the Data Controller's instructing party in a legal proceeding, or of witnesses or persons named in the case file). Legitimate interests of third parties: interest in the enforcement of claims and the settlement of disputes.

2.1.4. Duration of processing: personal data are usually processed by the Data Controller for 5 years from the completion/termination of the given order. For specific cases defined by law, see point 2.1.6 below.

2.1.5. Recipients: the Data Controller will only transfer personal data to third parties if this is necessary for the performance of the mandate. Data transfer may also be required by law, e.g. in the case of deposits by lawyers, the law requires the reporting of deposits to the Budapest Bar Association or, in certain cases, the Money Laundering Act requires reporting. For the legal requirements, see section 2.1.6 below.

2.1.6. Statutory processing of data relating to the activities of lawyers, scope of the data processed

2.1.6.1. Lawyers Act

2.1.6.1.1. Identification

The lawyer shall identify a natural person whom he does not know or whose identity is in doubt by inspecting his or her identity document or by applying the provisions of the Eüsztv. or, if the lawyer has the necessary conditions, by using the electronic identification service provided by the Government on a mandatory basis or by means of a check pursuant to Article 24(1)(a), (b) or (d) of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

In order to check the validity of the documents of natural persons and the consistency of the data contained in **the register** kept by the lawyer, the lawyer **is entitled to request the following data electronically from the register of identity and address data, the register of driving licences, the register of travel documents and the register of central immigration:**

- a) natural person identification data,
- b) citizenship, statelessness, refugee or EEA national status, long-term resident status,
- c) address,
- d) portrait,
- e) signature,
- f) the facts pursuant to paragraph (5) of Article 18 of Act LXVI of 1992 on the Registration of Personal Data and Addresses of Citizens,
- g) data pursuant to Section 24 (1) f) of Act XII of 1998 on Travel Abroad and the period of validity of the document,
- h) the data pursuant to Section 8 (1) (b) (ba)-bb) of Paragraph (1) (b) of Article 8 of Act LXXXIV of 1999 on Road Traffic Register,
- i) the data pursuant to Article 76 (d), Article 80 (1) (b) and (c) of Act I of 2007 on the Entry and Residence of Persons with the Right of Free Movement and Residence, and Article 254 (1) (g), Article 256 (1) (f) and Article 261 (1) (b) and (c) of Act XC of 2023 on the General Rules for the Entry and Residence of Third-Country Nationals.

If the natural person client is represented by a proxy, the lawyer may waive the need to identify the client separately if the power of attorney containing the client's details

- is countersigned by a lawyer,
- by a notary,
- the signature of the authorised representative has been notarised,
- or the power of attorney has been authenticated or recertified by the competent Hungarian diplomatic mission or consular post of the place of signature, or has been certified by an Apostille certificate.

If the lawyer is acting as a legal representative in proceedings for registration in a public register or drafting a document for registration in a public register, the natural person's data **must be retrieved** from the register.

2.1.6.1.2. Register of transactions requiring mandatory legal representation

The lawyer must keep a register of transactions requiring mandatory legal representation. The register of identified natural persons shall contain the following information:

- natural person identification data,
- address,
- citizenship, statelessness, refugee or EEA national status, long-term resident status,
- the type and number of the identification document used for identification,
- the identifier of the response received when requesting data from the register,
- case identifier for cases where the identification of the natural person is mandatory,
- data specified in the Act on the Prevention and Combating of Money Laundering and Terrorist Financing.

The register of identified legal entities and other entities contains the following personal data:

- the natural person identification data of the identified legal entity or person acting on behalf of another entity,
- data specified in the Act on the Prevention and Combating of Money Laundering and Terrorist Financing.

The lawyer is obliged to keep **changes to the** data in the register in such a way that the previous data remain available.

The Data Controller shall process the data of the above records for the period specified in the Money Laundering Act (8 years).

2.1.6.1.3. Conversion of a paper document into an electronic document

In certain cases specified by law, a lawyer may prepare an electronic document from a paper document. In such cases, the **electronic deed** must be kept for **10 years** and the **paper deed for 5 years, unless** the parties agree to a longer period.

2.1.6.1.4. Processing of legal deposits

The lawyer **shall record the** details of deposits exceeding twice the amount of the statutory minimum wage he/she manages and any changes thereto in the **electronic deposit register operated by the regional bar association.**

It must be recorded in the electronic deposit register:

- the name and bar number of the depositary lawyer,
- the case identifier of the escrow agreement,
- the type of deposit,
- the subject of the deposit,
- if the custodian lawyer places the deposit in a sub-account, the sub-account number,

- in the case of a deposit of money, the amount and currency of the money actually deposited,
- the date of conclusion, amendment or termination of the deposit contract,
- the date on which the data were recorded in the custody register and the date on which the recorded data were modified.

The data and any changes thereto shall be **recorded by the lawyer within one working day of the conclusion of the escrow agreement or any change in the data by means of a qualified electronic signature and an electronic declaration with a time stamp**. The electronic record shall assign a unique identification number to the deposit.

The electronic deposit record will **contain** the data for **10 years** after the termination of the deposit contract.

2.1.6.1.5. Case records and document management

The lawyer **must keep a record of the cases handled on the basis of the mandate**, in order to ensure that compliance with the rules governing the practice of the profession of lawyer can be verified and to protect the rights of clients in the event of the termination of the right to practise as a lawyer.

The register of cases **contains the** following data:

- the case identifier provided by the lawyer,
- the name of the customer,
- the subject of the case,
- the date on which the contract of engagement was concluded, and
- the registration number of the court proceedings relating to the case or the file number of other proceedings.

The lawyer **shall keep the data for 5 years after the termination of the mandate, for 10 years after the countersigning of the deed in the case of countersigning a deed, and for 10 years after the registration of the right to real estate in the public register**.

The register **may be consulted and requested** only by the staff or body carrying out the official control of the Bar and, in order to protect the rights of the client, by the deputy lawyer and the designated registrar.

The lawyer **shall keep the deed countersigned by him or her and other documents relating to the matter for which the deed was countersigned for 10 years from the date of countersignature, unless a longer period is provided for by law or the parties have agreed to keep them for a longer period**.

In the event of **the termination or cancellation of his/her membership of the Bar**, or of his/her deletion from the Bar Register, the **lawyer** shall ensure that the documents handled by him/her which cannot be discarded are handed over to the client or to another lawyer practicing legal activities in the given matter and authorized to handle the documents, and that the records are kept in accordance with the Lawyers Act.

2.1.6.2. Money Laundering Act.

2.1.6.2.1. Customer due diligence

The Money Laundering Act **requires lawyers to disclose information to clients in the following cases:**

- if they perform fiduciary activities,
- if they carry out custody of money and valuables
- if he/she performs activities as a lawyer under the Lawyers Act in connection with the preparation and execution of the following transactions:
 - the transfer of ownership of a share in a company or other business entity,
 - transfer of ownership of real estate,
 - the establishment, operation or dissolution of a company or other business entity;
 - a trust deed or unilateral declaration to establish a trust
 - the transfer without consideration of movable assets, in particular funds or financial assets.

Measures to verify the identity of the customer

- In the case of natural persons, the Data Controller shall record the identity of the natural person:
 - surname and given name,
 - surname and given name at birth,
 - citizenship,
 - place and date of birth,
 - mother's maiden name,
 - address or, in the absence thereof, place of residence,
 - the type and number of identification document;
- In the case of a legal entity or entities without legal personality, the Data Controller is required to record the following personal data (the other data to be recorded in such cases relate to the organisations):
 - the names and positions of the authorised representatives,
 - the identity of the delivery agent.

The lawyer must require the presentation of the following documents to verify identity:

- In the case of a natural person:
 - in the case of **Hungarian citizens**, **their** official identity card and official proof of permanent address,
 - in the case of **foreign nationals**, **their** travel document or identity card, provided that it entitles them to reside in Hungary, their document certifying their right of residence or their document entitling them to reside in Hungary,
- In the case of a legal entity or an entity without legal personality, a person authorised to act on its behalf or on based on its mandate:
 - in the case of **Hungarian citizens**, **their** official identity card and official proof of permanent address,

- in the case of **foreign nationals**, their travel document or identity card, provided that it entitles them to reside in Hungary, their document certifying their right of residence or their document entitling them to reside in Hungary.

The lawyer is required to **make copies of the** documents and certificates presented.

- Rules on proof of beneficial ownership

The natural person client must make a written declaration by personal appearance, in a manner determined by the supervisory authority, by means of a pre-audited electronic communication medium, that **he is acting on behalf or in the interest of the beneficial owner**.

- What information is the lawyer required to include in this declaration about the beneficial owner?
 - surname and given name
 - surname and given name at birth
 - citizenship
 - place and date of birth
 - address, or in the absence of an address, place of residence
- The lawyer is also required to ask the client whether the beneficial owner is considered a politically exposed person.

The representative of a client of a legal entity or an entity without legal personality must make a written declaration in person, in a manner determined by the supervisory body, by means of a pre-audited electronic communication medium, that **he or she is acting on behalf of or in the interest of the beneficial owner**.

- What information must the lawyer record in this declaration about the beneficial owner?
 - surname and given name
 - surname and given name at birth
 - citizenship
 - place and date of birth
 - address, or in the absence of an address, place of residence
 - the nature and extent of the ownership interest
- The lawyer is also required to ask the client whether the beneficial owner is considered a politically exposed person.

In what cases can proof of beneficial ownership be waived?

If, on the basis of a risk-sensitive approach, the lawyer records the data on the basis of the documents presented to him or her, as well as on the basis of the beneficial ownership register and other registers from which the lawyer is entitled by law to request data. (However, in such cases, the lawyer must also record the fact of the waiver.)

2.1.6.2.2. Measures relating to business contact and transaction data

The lawyer **must record the** following information about the business relationship:

- the type, subject and duration of the agreement,

- in order to determine the type of due diligence to be carried out on the client, whether the client's risk level is average, high or low,
- information about the purpose and intended nature of the business relationship,
- the circumstances of performance (place, time, method).

The lawyer is required to record the following information about the business relationship:

- the subject and amount of the mandate,
- the circumstances of performance (place, time, method).

On the basis of a risk-sensitive approach, the lawyer requests the provision of information on the **source of funds** and the production of documents relating to the source of funds in order to verify this information.

The lawyer must ensure that the available data and documents concerning the client and the determination of the client's risk level are up to date, in particular, in the event of becoming aware of a change in the available data and documents concerning the client, for the purpose of verifying the data on the beneficial owner under the law or for the purpose of fulfilling the cooperation in the field of taxation, the lawyer must check the available data on his client.

The monitoring obligation is to be carried out by the service provider on the basis of a risk-sensitive approach, annually in the case of high risk and at least every five years in the case of low risk. If, in the course of the verification, the provider has doubts as to the accuracy of the data and declarations, it shall repeat the customer due diligence measures necessary to eliminate the doubts.

In the event of a change of data, the lawyer only needs to carry out the client due diligence necessary to record the changed data, unless the full due diligence obligation applies.

When is a check required to be carried out to verify the identity of the customer and the beneficial owner?

As a general rule, it must carry out identity verification of the customer and the beneficial owner before establishing the business relationship, and may **exceptionally** do so during the business relationship if this is necessary to avoid disruption to the normal course of business and if the likelihood of money laundering or terrorist financing is low. In this case, the verification of identity shall be completed before the first transaction is concluded.

Client due diligence measures do not need to be repeated if

1. the lawyer has already carried out the client due diligence measures in relation to the client and the client's agent, nominee or representative acting on behalf of the service provider in connection with another business relationship or transaction,
2. has established the identity of the customer and the client's agent, nominee and representative acting on behalf of the service provider in connection with this business relationship or transaction; **and**
3. no change in the data.

Targeting, record keeping, statistics

Personal data (including information on the source of funds and assets) **obtained by the data controller in the course of customer due diligence** may be **accessed and processed by the data controller**, other than the lawyer, only for the purposes of the performance of its tasks in the prevention and combating of money laundering and terrorist financing and to the extent necessary for the performance of those tasks:

- the Head of Data Controller,
- helping family member,
- employee of the Data Controller.

How long must we retain data processed under the Money Laundering Act?

One is entitled and obligated to retain the data required by law (this applies to personal data, data that does not constitute personal data, documents and copies thereof) for **8 years** from the termination of the business relationship or the execution of the transaction.

The lawyer **is also required to record in the register transaction orders executed in cash (in HUF or in foreign currency) for an amount of HUF 4 million to HUF 500,000 or more**, which information must be kept for **8 years**.

At the request of a supervisory authority, the financial information unit, the investigative authority, the public prosecutor's office and the court, it must be kept for the period specified in the request, but not longer than **10 years** after the business relationship has ended or the transaction has been completed.

An extension on the basis of a request is possible only if the information or document specified therein is necessary for the purposes of ongoing or future proceedings. After this period has expired, it must be deleted or destroyed **without delay**.

2.2. NEWSLETTER SENDING

2.2.1. Data subjects: persons requesting the newsletter of the Data Controller, contact persons of the Data Controller's customers.

2.2.2. Purpose of data processing: to inform about changes in legislation, to provide professional news, articles, publications, information about the events of the Data Controller.

2.2.3. Data processed: name, e-mail address.

2.2.4. Legal basis for processing: consent of those who have requested the newsletter of the Data Controller. The legal basis for processing may also be the legitimate interest of the Data Controller. Legitimate interest: direct marketing (see recital 47 of the GDPR). The Data Controller will at all times provide the possibility to object (unsubscribe) (see below), so if the Data Subject declares that he/she does not wish to receive newsletters from the Data Controller, his/her data will be deleted by the Data Controller (unless there is another legal basis for processing them) and will not be used for this purpose after receipt of the request.

2.2.5. Duration of processing: until the Data Subject objects or until the previously given consent is withdrawn

2.3. CONTACTING, COMPLAINT HANDLING, REQUESTING A QUOTE

- 2.3.1. **Data subjects:** natural persons contacting the Data Controller, requesting a fee quote, enquiring or making a complaint, as well as natural persons contacting such undertakings.

Please be informed that pursuant to Section 194/A of the Lawyers Act, the internal whistleblowing system for lawyers, European Community lawyers, law firms and European Community law firms provided for by Act XXV of 2023 on complaints, whistleblowing and rules relating to the reporting of abuse (hereinafter: Whistleblowing Protection Act) is operated by the Hungarian Bar Association (hereinafter: MÜK).

You can access the information here:

https://www.mük.hu/_files/ugd/be2242_cee47693938f4e8b9558202da5fc6047.pdf

You can make a notification under the Whistleblower Protection Act here:

<https://www.mük.hu/panaszbejelentes>

- 2.3.2. **Purpose of processing:** in the event of contact by the Data Subject, the purpose of processing depending on the purpose of the contact (e.g. replying to enquiries received by filling in a contact form, preparing a quotation, replying to incoming e-mails, dealing with the substance of a complaint and informing about the action taken, etc.)
- 2.3.3. **The data processed:** name (filling in the contact form on the Data Controller's website is mandatory), e-mail address (filling in the contact form on the Data Controller's website is mandatory), telephone number, address (depending on the data communicated by the Data Subject or the channel of communication), company name and position, if applicable, and other data provided in the request.
- 2.3.4. **Legal basis for processing:** legitimate interest and processing necessary for the preparation of the agreement in case of a request for a quotation. Legitimate interest: ex-post verifiability of customer communications, complaint handling, quality assurance.
- 2.3.5. **Duration of data processing:** depending on the nature of the communication or complaint, but in any case for at least 5 years after the complaint has been dealt with.

2.4. STAFF SELECTION

- 2.4.1. **Data subjects:** persons applying for a job at the Data Controller or selected in connection with a specific job advertisement.
- 2.4.2. **Purpose of data processing:** the purpose of data processing until the application is assessed is to assess the applicant's professional suitability for the position advertised. Where the specific purpose of the collection of personal data is different, it will be explicitly indicated in the line below. The purposes of the processing after the assessment of the application are: (i) to keep the files necessary to prove the position of the Data Controller in the event of a claim by the applicant (legal basis for the latter processing: legitimate interest, see the information on this in the section "Legal basis for processing"), (ii) and, if the applicant specifically consents, direct inquiries by the Data Controller for the purpose of making further job offers.
- 2.4.3. **Scope of data processed:**
- Name, date and place of birth, nationality, permanent address, place of residence (purpose of data processing: identification of the applicant)
 - Telephone number, e-mail address (purpose of data processing: contact)
 - Details of the position applied for
 - Data on educational attainment

- Data on professional experience
- Data on language skills
- Skills, abilities
- If required: CV and the information contained therein, e.g.
 - portrait, if it is included in the CV
 - natural identity data (name, sex, date and place of birth, nationality)
 - language skills, educational and other qualifications, professional experience, preferred position, field of interest
 - the type of driving licence, if applicable, and any other information contained in the CV.
- If applicable: cover letter and its contents.

2.4.4. Legal basis for processing:

- The applicant's consent. Please note that you are not obliged to give your consent. However, if you do not consent to the processing of your data for recruitment purposes, we will not be able to consider your application. If you have given your consent, you may withdraw it at any time without giving any reason, but such withdrawal will not affect the lawfulness of the processing that took place before the withdrawal.
- The legal basis for the processing of data after the assessment of the application is the legitimate interest of the controller (legitimate interest: preservation of evidence in case of possible claims by the applicant, ex post verifiability of the lawfulness of the controller's actions), unless the applicant has given consent to further requests.

2.4.5. Duration of processing:

- In the event of an unsuccessful application, 12 months after the date of the decision on the application.
- If the applicant has given his/her consent, the data will be kept and used for a further 2 years in order to contact the applicant for the purpose of considering further job offers.
- In the event of a successful application, the data controller will process the data provided at the time of application only to the extent necessary for the establishment and maintenance of the employment relationship, in accordance with the separate information to be provided to employees.

2.5. TRAINEESHIP PROGRAMME

2.5.1. Data subjects: law students who are completing their compulsory university internship at the Data Controller.

2.5.2. Purpose of data processing: to provide traineeship opportunities, to identify the trainee, to provide the trainee with appropriate tasks, to maintain contact, to issue a certificate of traineeship.

2.5.3. Scope of data processed:

- Name, date and place of birth, nationality, permanent address, place of residence (purpose of data processing: identification of the applicant)
- Telephone number, e-mail address (purpose of data processing: contact)
- Information concerning language skills (for candidates applying for an intellectual job)
- Skills, abilities
- If required: CV and the information contained therein, e.g.
 - portrait, if it is included in the CV
 - natural identity data (name, sex, date and place of birth, nationality)
 - language skills, educational and other qualifications, professional experience, preferred position, field of interest

- the type of driving licence, if applicable, and any other information contained in the CV.
- If applicable: cover letter and its contents.

2.5.4. Legal basis for processing: consent of the Data Subject

2.5.5. Duration of data processing: 5 years from the end of the employment, unless the Data Subject's data (e.g. name) is stored on a data medium which the Data Controller is obliged to keep for a longer period.

3. Data processing

- 3.1.** A data processor is a natural or legal entity or any other body that processes personal data on behalf of the Data Controller. A processor may not take any substantive decision regarding the processing, may process personal data of which it becomes aware only in accordance with the provisions of the Data Controller, may not process personal data for its own purposes and shall store and retain personal data in accordance with the provisions of the Data Controller.
- 3.2.** The Data Controller may occasionally involve translators, legal experts or subcontractors of lawyers, tax advisors, financial advisors in the performance of the mandate. These persons are considered as processors for the purposes of processing personal data. You can request information on the specific identity of the processors by contacting the Data Controller.

4. Data security

- 4.1.** The Data Controller shall ensure the security of the data in accordance with the applicable regulations. The Data Controller shall, among the measures relating to data security, in particular take technical and organisational measures and establish procedural rules to ensure that the data processed are protected against unauthorised access, alteration, disclosure, transmission, disclosure, erasure, destruction, accidental destruction or damage and against inaccessibility resulting from changes in the technology used.
- 4.2.** The Data Controller shall take into account the state of the art of technology when determining and applying data security measures. Among several possible processing solutions, the Data Controller shall choose the one which ensures a higher level of protection of personal data, unless this would impose a disproportionate burden on the Data Controller. The Data Controller shall also enforce these requirements vis-à-vis processors.
- 4.3.** The Data Controller provides different levels of access rights within the software used, according to the user hierarchy. In order to avoid the loss of data, the contents of computers and servers are backed up. IT systems are protected by appropriate firewalls. The Data Controller shall ensure adequate virus protection of the IT system. The Data Controller shall provide its employees with appropriate training on data security requirements. The Data Controller shall maintain strict standards for the activities of the data processors it uses.
- 4.4.** The Data Controller undertakes to require any third party to whom it may transfer or disclose the data to comply with the above undertakings. However, in the event of a lawful transfer of data by the Data Controller, the Data Controller shall not be liable for any damage caused by the recipient.
- 4.5.** All employees of the Data Controller, by virtue of their employment or other legal relationship, are obliged to comply with the above principles on data processing and data security.

4.6. DATA PROCESSING AS A WHISTLEBLOWER PROTECTION LAWYER

4.6.1. Data subjects: our law firm provides whistleblower protection legal services under the Whistleblower Protection Act to the organisations that engage our law firm. In such cases, our law firm handles the reporting of whistleblower violations or other misconduct to the relevant organizations under the Whistleblower Protection Act.

Data subjects are the whistleblower on the one hand, and the person concerned by the notification on the other (the person whose conduct or omission gave rise to the notification and the person who may have material information about the facts contained in the notification). Other persons concerned may be those who are interviewed during the investigation of the notification or whose personal data are included in the evidence obtained. Contact persons of the organisation are also concerned.

Data subjects typically have or have sought to have a legal relationship with the organisation in question or have had such a relationship in the past. For more information on what legal relationships can be reported, see the organisation's general information on the whistleblowing system and the list in Section 20 of the Whistleblowing Protection Act.

4.6.2. Purpose of processing:

Under the Whistleblower Protection Act, the internal whistleblower reporting system is available to (a) the whistleblower, (b) the person whose conduct or omission gave rise to the whistleblowing, and (c) the person who may have material information about the matters contained in the whistleblowing, personal data essential to the investigation of the notification may be processed only for the purposes of investigating the notification and remedying or stopping the conduct that is the subject of the notification and may be disclosed to the whistleblower protection lawyer or to an external body involved in the investigation of the notification.

4.6.3. Scope of data processed:

In running the whistleblowing system, we process the name and contact details of the whistleblower (if provided by the whistleblower) in order to keep in contact with the whistleblower and provide feedback on the investigation of the whistleblowing. We also process the personal data contained in the notification. This includes the names, titles and other details of the persons concerned by the notification, as set out in the content of the notification. In the course of the investigation of the notification, we may also need to process other personal data that are relevant to the subject matter of the notification, such as job title, salary, work schedule, duties, email address, telephone number, and other personal data related to the facts alleged in the notification. During the investigation of the notification, we may interview individuals and obtain additional evidence for the purpose of investigating the merits of the notification. A record of the interviews will be kept. If the whistleblower provides us with photographs, audio or video recordings as part of the notification and knowledge of these is indeed necessary for the investigation of the notification, we will also process these data for the purposes of the investigation.

Personal data is obtained from the notification and information is also obtained from the interviewees during the investigation. During the investigation, we may collect additional evidence, typically consisting of data and documents contained in the internal records of the organisation concerned.

If the whistleblower makes a report over a recorded telephone line, we will handle the recorded audio material on the basis of his or her consent.

- 4.6.4. **Legal basis for processing**: the legal basis for processing is the fulfilment of legal obligations to investigate notifications. If the whistleblower makes the report orally by calling a recorded telephone line, the legal basis for the making and processing of the audio recording is the consent of the whistleblower.
- 4.6.5. **Duration of data processing**: under the Whistleblower Protection Act, data and documents relating to the notification, the investigation and the action taken must be kept for 5 years from the end of the action.

5. Rights of data subjects in relation to the processing of their personal data

- 5.1. The Data Subject may, at any time, **request information** about the processing of personal data concerning him or her, request the rectification, erasure or restriction of the processing of personal data concerning him or her, and object to the processing of such personal data, using the contact details indicated in this notice. The Data Subject also has the right to data portability.
- 5.2. The Data Controller **shall inform the** Data Subject of the **action taken on the request** without undue delay, but in any event within one month of receipt of the request. If necessary, taking into account the complexity of the request and the number of requests, this time limit may be extended by a further two months. The Data Controller shall inform the data subject of the extension of the time limit, stating the reasons for the delay, within one month of receipt of the request. If the request has been made by electronic means, the information shall also be provided by electronic means where possible, unless the Data Subject requests otherwise. If we consider that we do not need to take action on the Data Subject's request, we will inform the Data Subject without delay, but at the latest within one month of receipt of the request, of the reasons for non-action and of the possibility to lodge a complaint with the DPA and to exercise his or her right to judicial remedy.
- 5.3. The execution of requests shall be free of charge, but if the request is manifestly unfounded or excessive, in particular because of its repetitive nature, the Data Controller may charge a reasonable fee, taking into account the administrative costs incurred as a result of the request, or refuse to execute the request.
- 5.4. If there is reasonable doubt about the identity of the Data Subject submitting the request, additional information necessary to confirm his or her identity may be requested.
- 5.5. At the Data Subject's request, the Data Controller shall provide information on whether or not his or her personal data are being processed and, if so, the Data Subject shall have the right to obtain access to the personal data relating to him or her which are processed by the Data Controller, as well as information on the purposes of the processing, the categories of data concerned, the recipients or categories of recipients to whom the personal data have been or will be disclosed, the envisaged duration of the processing or the criteria for determining the duration of the processing, and the source of the data.
- 5.6. Upon request, the Data Controller shall provide the Data Subject with a copy of the personal data processed. Additional copies requested by the Data Subject may be charged a reasonable fee based on administrative costs. If the Data Subject has made the request by electronic means, the information shall be provided in a commonly used electronic format, unless otherwise requested by the Data Subject.
- 5.7. The Data Subject **may request the rectification of inaccurate data and has** the right to request the completion of incomplete data.
- 5.8. The Data Subject **may request the Data Controller to erase the personal data** if.
- they are no longer necessary for the purposes for which they were processed;
 - if the Data Subject withdraws his or her consent and there is no other legal basis for the processing;
 - the Data Subject has objected to the processing and the conditions set out in point 5.13 apply;

- d) the processing is unlawful;
 - e) they must be deleted in order to comply with a legal obligation to which the Data Controller is subject,
 - f) the Data Subject is a minor under the age of 16.
- 5.9.** The Data Controller shall **delete the data upon such a request, unless** the further processing of the data is necessary for the purposes of
- a) exercising the right to freedom of expression and information,
 - b) complying with a legal obligation to which the Data Controller is subject,
 - c) bringing, asserting or defending legal claims.
- 5.10.** At the request of the Data Subject, **the Data Controller shall restrict processing** if.
- a) the Data Subject contests the accuracy of the personal data, in which case the restriction applies for the period of time necessary to allow the accuracy of the data to be verified,
 - b) although the processing is unlawful, the Data Subject opposes erasure and requests restriction instead,
 - c) the Data Controller no longer needs to process the data, but the Data Subject requires it for the establishment, exercise or defence of legal claims,
 - d) the Data Subject has objected to the processing in accordance with point 5.13, in which case the restriction applies for the period until it is established whether the legitimate grounds of the controller prevail over those of the Data Subject.
- 5.11.** If processing is restricted as described above, such personal data, with the exception of storage, may only be processed with the consent of the Data Subject or for the establishment, exercise or defence of legal claims or for the protection of the rights of another person or for important public interests of the Union or of a Member State. The Data Controller shall inform the Data Subject requesting the lifting of the restriction in advance.
- 5.12.** The Data Controller shall notify the Data Subject of the rectification, erasure or restriction, as well as all those to whom the data were previously disclosed. The Data Controller shall refrain from such notification where it is impossible or would require a major effort. If the Data Controller has disclosed the personal data and is required to delete it, it shall take reasonable steps, including technical measures, taking into account the available technology and the cost of implementation, to inform other controllers that process the data that the Data Subject has requested them to delete the links to or copies or replicas of the personal data in question.
- 5.13.** **The Data Subject may object to the processing of their personal data,**
- (a) if it is based on legitimate interest, in which case the processing shall not be carried out unless it is justified by compelling legitimate grounds which override the interests, rights and freedoms of the Data Subject or for reasons relating to the establishment, exercise or defence of legal claims,
 - (b) if it is carried out for the purposes of, or in connection with, direct marketing; in such a case, the processing may no longer be carried out for such purposes.
- 5.14.** On the basis of the **right to data portability**, the Data Subject may, on the one hand, request the Data Controller to provide him or her with his or her personal data processed in a structured, commonly used, machine-readable format, where technically feasible, and to transmit it to any controller, and on the other hand, request the Data Controller to transmit his or her data.
- 5.15.** If the Data Controller does not comply with the Data Subject's request as set out above, the Data Controller shall inform the Data Subject of the reasons for the failure within one month of receipt of the request at the latest.

5.16. If the Data Subject believes that his or her rights in relation to his or her personal data have been infringed, he or she is requested to notify the Data Controller of his or her complaint using one of the contact details provided below.

5.17. You may also apply to the public authority regardless of the notification by the Data Controller. If you so decide, you can notify the authority using the contact details below:

National Authority for Data Protection and Freedom of Information
Address: 1055 Budapest, Falk Miksa utca 9-11
Postal address: 1363 Budapest, PO Box 9.
Phone: +36 -1-391-1400
Fax: +36-1-391-1410
E-mail: ugyfelszolgalat@naih.hu

5.18. If you experience unlawful processing, you can also bring a civil action. The court has jurisdiction to hear the case. You can also bring the case before the court in your country of residence (for a list of courts and their contact details, please see the following link: <http://birosag.hu/torvenyszekek>).

6. **Changes to the privacy notice** will be published on the website of the Data Controller. The Data Protection Notice currently in force shall always apply to the processing of personal data, even if an earlier data protection notice was in force at the time of registration or other provision of personal data by the Data Subject.

7. Contact

7.1. If you have any questions, comments or requests about this privacy notice, or if you wish to make a complaint or exercise any of the rights set out above, please contact us using one of the contact details provided at the beginning of this notice.