

Data processing related to the operation of the website on privacy notice

Uzsoki Law Firm (hereinafter: „Controller”), related to the data processing activity in connection with the operation of the www.druzsoki.hu website, discloses the following information to the data subjects based on Articles 13 and 14 of *REGULATION (EU) 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, and repealing Directive 95/46/EC (General Data Protection Regulation)* (GDPR).

Definitions

- *data subject*: any specified **natural person**, directly or indirectly identified or identifiable based on personal data.
- *personal data*: data which could be attributed to the data subject, any information relating to the identified or identifiable natural person (“data subject”), in particular the name, identifier and one or more information on physical, physiological, mental, economic, cultural or social identity, and conclusion that can be drawn thereof regarding the data subject. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- *sensitive data*: data revealing racial or ethnic origin, political opinion, party affiliation, religion or beliefs, party membership, health status, pathological addiction, sexual life, sexual orientation.
- *data set*: all data processed in a single file.
- *criminal personal data*: personal data relating to the data subject or that pertain to any prior criminal offense committed by the data subject and that is obtained by organizations authorized to conduct criminal proceedings or investigations or by penal institutions during or prior to criminal proceedings in connection with a crime or criminal proceedings.
- *consent*: any freely and expressly given specific and informed indication of the will of the data subject by which he/she signifies his/her agreement to personal data relating to him/her being processed fully or to the extent of specific operations.
- *objection*: the statement of the data subject by which he/she objects to the processing of his/her data, and requests the termination of processing or the erasure of the processed data.
- *controller*: natural or legal person, or organisation without legal personality which alone or jointly with others determines the purposes and means of the processing of data; makes and executes decisions concerning data processing (including the means used) or have it executed by a data processor.

- *processing*: any operation or the totality of operations performed on the data, irrespective of the procedure applied; in particular, collecting, recording, registering, classifying, storing, modifying, using, querying, transferring, disclosing, synchronising or connecting, blocking, deleting and destructing the data and the prevention of further use of the data.
- *data transfer*: ensuring access to the data for a third party.
- *disclosure*: ensuring open access to the data.
- *data deletion*: making data unrecognisable in a way that it can never again be restored.
- *tagging data*: marking data with a special ID tag to differentiate it.
- *restriction*: marking data with a special ID tag to indefinitely or definitely restrict its further processing.
- *data destruction*: complete physical destruction of the data carrier recording the data or the execution of an unrecoverable process made on the data carriers containing data.
- *data processing*: performing technical tasks in connection with data processing operations, irrespective of the method and means used for executing the operations, as well as the place of execution, provided that the technical task is performed on the data.
- *processor*: any natural or legal person or organisation without legal personality processing the data on the grounds of a contract, including contracts concluded pursuant to legislative provisions.
- *filing system*: any structured set of data functionally centralised, decentralised or dispersed on geographic basis which are accessible according to specific criteria.
- *third person*: any natural or legal person, or organisation without legal personality other than the data subject, the data controller or the data processor.
- *Hungarian National Authority for Data Protection and Freedom of Information*: Its legal status and tasks are specified by Section 38 of the Privacy Act (hereinafter: Authority or NAIH).
- *contracting partner*: Any natural or legal person that concluded a contract with Dr Tibor Csaba Takács.
- *identification data regarding natural persons*: The family and given name, name at birth, mother's name, place and date of birth of the data subject.
- *URL*: Uniform Resource Locator, standardised address of certain resources (e.g. texts, images) that can be found on the Internet. Uniform resource locator, standard system for addressing used on the Internet, it provides the method of accessing information and the exact location of the information on a remote computer.
- *personal data breach*: unlawful processing of personal data, in particular the unauthorised access, alteration, transfer, disclosure, deletion or destruction and accidental destruction and breach.

Data of the Controller

Name of the controller	Uzsoki Law Firm
Registered office	H-1117 Budapest, Galvani utca 44.
Website	www.druzsoki.hu
Postal address	H-1117 Budapest, Galvani utca 44.
Email address	uzsoki@druzsoki.hu

Processed data

Description of the activity and the purpose of processing	Legal basis	Processed personal data	Time limit
Use of the Contact function Personal data provided during the use of the “Contact” menu shall be processed by the Controller exclusively for the purpose of responding to the request and to an extent necessary. Following the response to the request, if there is no need for further contact with the data subject, the data will be erased.	freely given consent	email address name	Until response to the request, however, for no longer than 1 year

The Controller transfers the processed personal data in cases specified by legislation, at the request of the authority, to the proper authority or body for compliance with legal provisions.

PRINCIPLES OF PROCESSING

During processing by the Controller, it follows the following principles in compliance with the GDPR:

- **Lawfulness, fairness and transparency:** personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject. According thereto the Controller processes personal data which are necessary for carrying out its tasks and which are suitable. The Controller erase all data for which the processing purpose has been terminated or for the processing of which the data subject has withdrawn his/her consent, or for the processing of which it has no legal basis pursuant to legislation.
- **Purpose limitation:** personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

According thereto the Controller processes personal data which are necessary for carrying out its tasks and which are suitable.

The personal data processed must be essential for the purpose for which it was recorded, and it must be suitable to achieve that purpose. Personal data may be processed to the extent and for the duration necessary to achieve its purpose.

The data subject, at his/her request, must be informed of all activities related to the processing of his/her data *clearly and in details*, in particular regarding the source of the data processed by the Controller, the purpose and legal basis of the processing, the name, address of the person(s) authorised for processing, the period of processing, and whether the controller processes his/her personal data in compliance with the effective regulations, and regarding who may become familiar with the data, and, in the case of transferring the personal data of the data subject, the legal basis of the transfer and the recipient. The information shall cover the rights and available remedies of the data subject related to the processing.

The Controller shall ensure that only those processors access the data that regarding their processing the principle of purpose limitation can be considered realised.

- **Data minimisation:** personal data shall be adequate, relevant and limited to what is necessary and sufficient in relation to the purposes for which they are processed. With regard to the purpose of processing the narrowest range of personal data will be processed by the Controller where appropriate. The Controller shall provide in connection with the principle of data minimisation that based on the data identification of the relevant person is only possible until the realisation of the purpose of processing. This shall mean the limitation of the storage period of the data. The requirement of purpose limitation and data minimisation shall cover each stage of processing, including data transfer as well.
- **Accuracy:** personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken by the Controller to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- **Storage limitation:** personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.
- **Integrity and confidentiality:** personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. The Controller shall take all the necessary measures from the point of view of information technology, and from technical and legal perspective to protect the personal data.

The Controller shall ensure that the processing carried out by it complies with the requirements of fairness and lawfulness and the complete and up-to-date processing; it shall also ensure that the data are accessible to both the data subjects and the authorised persons and that the data are not accessible to unauthorised persons.

RIGHTS OF THE DATA SUBJECT

Natural persons involved in processing shall have the following rights in connection with processing:

1. Requesting information, access:

The data subjects shall have the right to obtain from the Controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

- a) the purposes of the processing;
- b) the categories of personal data concerned,
- c) the recipients to whom the personal data have been or will be disclosed,
- d) the envisaged period for which the personal data will be stored,
- e) information on the right to request rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing
- f) the right to lodge a complaint,
- g) existence of automated decision-making based on your personal data, including profiling, and information about the logic involved, as well as the significance and the envisaged consequences of such processing for you.

The Controller shall provide information within one month of receipt of the request without undue delay. The Controller shall respond in a form identical to the way the data subject established its request for information.

The first information provided shall be free of charge in the relevant calendar year. Request for information on the same set of data again shall be charged with an administration fee by the Controller, provided that during the repeated request for information no infringement took place and there was no rectification of the data.

The chargeable fee is gross HUF 1,000 per involved data.

2. Rectification

If the personal data processed by the Controller is inaccurate and the accurate personal data is available, he/she shall send it to the Controller and the Controller shall rectify the personal data.

3. Erasure of your personal data

The Controller shall erase the processed personal data if

- a) its processing is unlawful;
- b) the data subject withdraws consent and there is no other legal ground for the processing;
- c) the data subject objects to the processing;
- d) there is no longer need for the processing for the purpose for which the data was collected;
- e) the personal data have to be erased in order to comply with the legislation.

4. Restriction of the processing of personal data

Restriction of processing may take place in the following cases:

- a) if the accuracy of the personal data processed by the Controller is contested by the data subject (in such case, for a period enabling the Controller to verify the accuracy of the personal data);
- b) if the processing is unlawful and the data subject, instead of erasure of the personal data, requests the restriction of their use instead;
- c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims.
- d) the data subject objects to processing (pending the verification whether the legitimate grounds of the controller override those of the data subject).

During the restriction of the processing, the Controller shall not carry out any processing activity other than storage. The data subject shall be informed by the Controller before the restriction of processing is lifted.

5. Objection

The data subject shall have the right to object to processing his/her data for direct marketing purposes. The data subject may communicate his/her objection based on the information provided in the newsletter by clicking on the link therein.

6. Complaint

If the data subject considers prejudicial to him/her the processing by the Controller, he/she may lodge a complaint to the Hungarian National Authority for Data Protection and Freedom of Information.

7. Right to data portability

The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to the Controller, in a structured, commonly used and machine-readable format.

8. Compensation and payment for damages

If the Controller causes damage to the data subject or others by the unlawful or unsafe processing of the personal data, the data subject or the aggrieved person shall have the right to enforce the compensation against the Controller. However, if the infringement affects the privacy rights of the data subject, he/she shall have the right to enforce payment of damages.

The Controller shall have no obligation for compensation or for payment of damages if the damage was incurred by an unavoidable external cause outside the scope of processing that can be proven, or if the damage is incurred due to the data subject's intentional or grossly negligent conduct.

LEGAL REMEDY

Response to personal data breaches

The Controller pays particular attention to detect the personal data breaches in due time to establish what occurred exactly, the severity of the data breach, and what effect could it have on the data subjects.

The Controller acknowledges that the personal data breach could, if not addressed in an appropriate and timely manner, cause physical, financial or non-financial damage to the natural persons. In order to manage the personal data breaches, the Controller keeps a record in which it records the circumstances of the personal data breach within 72 hours following the notification of the breach.

The task of the Controller in the case of a personal data breach:

- in the case of a personal data breach, the Controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent (NAIH); Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.
- when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.
- as the Controller, it records the personal data breaches.

The notification to the NAIH on the personal data breach shall:

- describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

- communicate the name and contact details of the contact point where more information can be obtained;
- describe the likely consequences of the personal data breach;
- describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

General legal remedy

The affected person may receive information on the processing of his/her personal data from the Controller and may request the rectification and erasure of his/her personal data upon prior appointment from Monday to Friday between 10 a.m. and 4 p.m. without voice recording. The Controller investigates the complaint within the shortest possible time from the request but no later than 15 days and provides written information.

If the affected person does not agree with the decision or the information regarding the processing of personal data by the Controller or if the Controller fails to comply with the deadline of responding as specified in the legislation, the data subject may initiate proceedings at the court or the National Authority for Data Protection and Freedom of Information within 30 days from the failure to meet the deadline. The adjudication of the lawsuit falls within the jurisdiction of the court. If the court approves the request, it may oblige the Controller to give information, to rectify, block, erase the data, to destruct the decision made by automatic data processing, to take into consideration the data subject's right to object, or to release data.

The data subject may initiate proceedings at the National Authority for Data Protection and Freedom of Information in the case of any infringement.

Also, the data subjects may initiate proceedings at the court in the case of violation of their rights.

You may make a statement in the case of violation of the data subject's rights or in the case of a remark at the contact details below or initiate proceedings at the following authorities:

- Metropolitan Court of Budapest H-1055 Budapest, Markó u. 27.
- Contact details of NAIH: website:
- <http://www.naih.hu/>
- address: H-1055 Budapest Falk Miksa u. 9-11.
- postal address: H-1363 Budapest, Pf. 9.
- email: ugyfelszolgalat@naih.hu

If the data subject does not agree with the decision of the Controller made regarding processing or his/her rights are violated in any other way, the data subject may initiate proceedings at the court.

The case can be given priority by the court. The Controller shall reimburse the damages caused by the unlawful processing of the data subject or the damages caused to other persons by violating the requirements of data security.

Furthermore, at the Hungarian National Authority for Data Protection and Freedom of Information (<http://naih.hu/>; H-1530 Budapest, Pf.: 5.; phone: +36-1-391-1400; fax: +36-1-391-1410; email: ugyfelszolgalat@naih.hu), by notification, any person may initiate an investigation by referring to the fact that an infringement occurred or its imminent threat exists related to the processing of personal data or the exercise of rights regarding knowledge of public data or data of public interest.

Prior to the initiation of any proceeding it is recommended to send the complaint to the Controller.

Initiating proceedings at the court

We inform you, that you shall have the right to enforce your claim before the court. The adjudication of the lawsuit falls within the jurisdiction of the court. The lawsuit may be initiated at the court within the geographical area of our registered office or even you place of residence or place of habitual residence.