

## **PRIVACY NOTICE - itineris.hu**

### **1. INTRODUCTION**

Itineris Kft (hereinafter: 'ITineris Kft', 'Service Provider', 'Controller' or 'Company'), as Controller, acknowledges the content of this legal notice as binding.

The Company undertakes to ensure that all data processing related to its activity meets the requirements set out in this policy and in all applicable legislation.

Itineris Kft is the operator of websites <https://www.itineris.hu>, itineris.eu, wayquest.pl, wayquest.cz, wayquest.sk, wayquest.hu, utdijfizeto.hu, utdijfiz.hu.

Itineris Kft reserves the right to modify this Notice at any time. Naturally, notifying its audience of any changes in a timely manner.

Itineris Kft is committed to the protection of the personal data of its clients and partners, and considers it extremely important to respect the right of its clients to informational self-determination. The Controller processes personal data confidentially and implements all security, technical and organisational measures that guarantee the security of the data.

ITineris Kft describes its data processing principles below, and presents the expectations it has set for itself as a data controller, with which it complies. The processing principles are in line with the effective legislation on data protection, in particular, the following:

- Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information;
- Act V of 2013 on the Civil Code (hereinafter: 'Civil Code');
- Act XLVIII of 2008 on the Fundamental Conditions and Certain Limitations of Economic Advertising Activities (hereinafter: 'Grt.');
- Act CVIII of 2001 on E-commerce and Certain Issues Regarding Information Society Services (hereinafter: 'E-Commerce Act');
- Regulation of the European Parliament and of the Council (EU) 2016/679 (27 April 2016) on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and repealing Directive 95/46/EC (General Data Protection Regulation, hereinafter: '**GDPR**')

### **2. DEFINITIONS**

- data subject: a natural person who has been identified by reference to specific personal data, or who can be identified, directly or indirectly;
- personal data: data relating to the data subject, in particular by reference to the name and identification number of the data subject or one or more factors specific to his physical, physiological, mental, economic, cultural or social identity as well as conclusions drawn from the data in regard to the data subject;
- consent: any freely and expressly given specific and informed indication of the will of the data subject by which they indicate their express consent to their personal data being processed fully or to the extent of the specific operations;
- Controller: any 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 contracts a Processor to execute it;
- data management: 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, synchronizing or connecting, blocking, erasing and destroying the data, as well as preventing their further use, taking photos, making audio or visual recordings, as well as registering physical characteristics suitable for personal identification (such as fingerprints or palm prints, DNA samples, iris scans);
- data transfer: ensuring open access to the data to specific third parties
- disclosure: ensuring open access to the data to anyone;
- data erasure: making data unrecognisable in a way that it can never again be restored;
- data processing: a series of data control and technical activities, irrespective of the method or instrument used for the implementation of the tasks, or the place of application, providing that the technical activity is performed on the data;
- Processor: a natural or legal person or unincorporated organisation that is engaged under contract in the processing of personal data, including when the contract is concluded by virtue of law.

### 3. COMPANY DATA

The data and contact details of our Company are as follows:

Name:	<b>ITineris Informatikai Kft.</b>
Correspondence address:	1145 Budapest, Mexikói út 42/B
Company registration number:	01-09-739921
Tax number:	13527316-2-42
Phone number:	+36 20 491 9204
E-mail:	<a href="mailto:info@itineris.hu">info@itineris.hu</a>
Representative of the Controller:	Gábor Szilágyi - managing director

### 4. RANGE OF PERSONAL DATA, THE PURPOSE, LEGAL GROUND AND DURATION OF PROCESSING

Please note that if the data providers providing data to Itineris Kft. are providing the personal data of a third party, it is their obligation to obtain the consent of the data subject. The Controller is not obliged to check if these have been obtained. The Controller draws the partner's attention to the fact that if they do not fulfil this obligation, and as a result the data subject enforces a claim against the Controller, the Controller may pass on the enforced claim or the amount of related damages to the partner.

We provide the following information regarding each of our processings.

#### 4.1. Call for proposal, showing of interest through direct inquiry

Those interested have the opportunity to make a direct inquiry to our Company by e-mail sent to the Company's address ([info@itineris.hu](mailto:info@itineris.hu)) or by telephone.

**Purpose of data processing:**

Liaising to promote communication between the data subject and our Company, and to cooperate as closely and effectively as possible.

**Legal ground of data processing:** legitimate interest – Article 6 (1) f) of the GDPR

**Processed personal data:** name, e-mail address and phone number of the Contracting Authority/Contact Person and other information provided by the data subject,

**Duration of data processing:** until the proposal is valid or the objection of the data subject

**Recipients of the personal data:** The controller shall not provide the data obtained to third parties, with the exception of the processor(s) indicated in Section 7. The recorded data may be accessed only by the employees of the Controller and the designated employees of the processor(s).

**Indication of legitimate interest:** The legitimate interest of our company is to process the data of the data subject - direct business acquisition

**Data subjects affected by the data processing:**

The partners and data subject directly interested in the services of the Company (e.g.: by e-mail or telephone).

#### 4.2. Call for proposal, data processing related to its follow-up

**Purpose of data processing:** it is in the legitimate interest of the controller to record the data of the data subject for the purpose of direct business acquisition beyond the validity period of the proposal.

**Legal ground of data processing:** legitimate interest of the controller, Article 6 (1) f) of the GDPR,

**Processed personal data:** Contact person's surname and first name; telephone number; e-mail address

**Recipients of the personal data:** The controller shall not provide the data obtained to third parties, with the exception of the processor(s) indicated in Section 7. The recorded data may be accessed only by the employees of the Controller and the designated employees of the processor(s).

**Duration of processing:** until the objection of the data subject

**Indication of legitimate interest:**

Establishing business relations with partners and contracting authorities, accurate information, informing of data subjects. The legitimate interest of our company is to process the data of the data subject - direct business acquisition

**Data subjects affected by the data processing:**

The recipients of the proposals previously issued by the Company and the contact person(s) included therein.

#### 4.3. Processing of client contact details in client contracts (in the case of a legal person contracting party)

**Purpose of data processing:** processing the contact details of the contact person in the contracts concluded with the client; to facilitate fast, accurate, and effective communication with the client

**Legal ground of data processing:** legitimate interest – Article 6 (1) f) of the GDPR

**Processed personal data:** name, company e-mail address and phone number of the contact person

**Duration of processing:** for 8 years following the expiry of the contract

**Recipients of the personal data:** The controller shall not provide the data obtained to third parties, with the exception of the indicated processor(s). The recorded data may be accessed only by the employees of the Controller, the designated employees of the processor(s) and the contracted client and their employees.

**Indication of legitimate interest:** It is in the legitimate interest of our company to process the data of the data subject in a client contract (name, company e-mail address, telephone number). The client can communicate with the contact person the communication required to fulfil the contract through the specified communication channels.

**Data subjects affected by the data processing:**

The data subjects in the contract concluded between the Company and the client.

#### 4.4. Processing of client data in client contracts in the case of a private entrepreneur client/data subject

**Purpose of data processing:** processing the contact details of the contact person in the contracts concluded with the client, in order to ensure the successful receivables management process of the company

**Legal ground of data processing:** legitimate interest – Article 6 (1) f) of the GDPR

**Processed personal data:** private entrepreneur: - mother's name, - Name at birth, - Place of birth, Date of birth

**Duration of processing:** for 8 years following the expiry of the contract

**Recipients of the personal data:** The controller shall not provide the data obtained to third parties, with the exception of the indicated processor(s). The recorded data may be accessed only by the employees of the Controller, the designated employees of the processor(s) and the contracted client and their employees.

**Indication of legitimate interest:** It is in the legitimate interest of our company to process the data of the data subject in a client contract (private entrepreneur: -mother's name, -Name at birth, -Place of birth, -Date of birth). In order to submit any payment orders, in the case of an private entrepreneur, it is necessary to provide the above-mentioned data.

**Data subjects affected by the data processing:** The data subjects in the contract concluded between the Company and the client (only in the case of private entrepreneurs).

#### 4.5. Cattle breeder registration

**Purpose of data processing:** registration of a cattle breeder in the official system

**Legal ground of data processing:** fulfilment of contract / order - Article 6 (1) b) of the GDPR, according to legislation - Article 6 (1) c) of the GDPR.

**Processed personal data:**

- Name and contact details of the livestock breeder
- name and contact details of the contact person (in the case of a legal person)
- Billing address
- Invoice amount
- Purchased products, invoiced services
- for 8 years following the expiry of the contract

**Duration of processing:** until the deadline specified in the Accounting Act

**Possible consequences of the failure to provide the required data:** The provision of data is mandatory.

**Recipients of the personal data:** The controller shall not provide the data obtained to third parties, with the exception of the processor(s) indicated in Section 7. The recorded data may be accessed only by the employees of the Controller and the designated employees of the processor(s).

**Data subjects affected by the data processing:**

The data subjects with whom the Company is in a contractual relationship (cattle registration)

#### 4.6. CATTLE BREEDING AND FATTENING system registration (Beef)

**Purpose of data processing:**

The contracted partners have the opportunity to register on the electronic interface operated by the Company. The use of the webshop is subject to registration. When registering, the data subject creates an account.

The purpose of the data processing is to register and differentiate between customers.

**Legal ground of data processing:** voluntary consent - Article 6 (1) a) of the GDPR By checking the box on the website, you give your voluntary consent to the processing of your personal data, and the performance of a contract pursuant to Article 6 (1) b) of the GDPR.

**Processed personal data:**

- Registering person's (data subject)
  - username (provided by the user)
  - name
  - e-mail address.

**Duration of processing:** until the consent is withdrawn, until the deletion of the data subject's account, or until the expiry of the contract.

**Recipients of the personal data:** The controller shall not provide the data obtained to third parties, with the exception of the processor(s) indicated in Section 7. The recorded data may be accessed only by the employees of the Controller and the designated employees of the processor(s).

**Possible consequences of the failure to provide the required data:** If data are missing, the User will not be able to use their client account. The provision of the data is a prerequisite for the use of the service.

**Data subjects affected by the data processing:**

The data subjects who create an account in the system (Beef) operated by the Controller.

#### 4.7. Data processing related to the Beef client account

**Purpose of data processing:** Data processing related to the client account, user assignment

**Legal ground of data processing:** fulfilment of contract / order - Article 6 (1) b) of the GDPR

**Processed personal data:**

- Name and e-mail address of the user

**Duration of processing:** Until the expiry of the contract or until the user profile/client account is deleted by the data subject.

**Recipients of the personal data:** The controller shall not provide the data obtained to third parties, with the exception of the processor(s) indicated in Section 8. The recorded data may be accessed only by the employees of the Controller and the designated employees of the processor(s).

**Possible consequences of the failure to provide the required data:** If data are missing, the User will not be able to use their client account. The provision of the data is a prerequisite for the use of the service.

**Data subjects affected by the data processing:**

The data subjects using the account registration function, contracted partners of the Controller.

#### 4.8. Installation of on-board unit

**Purpose of data processing:** Data processing of documents created during the installation of the on-board unit

**Legal ground of data processing:** fulfilment of contract / order - Article 6 (1) b) of the GDPR

**Processed personal data:**

- The customer's (invoice payer)
  - name,

- place of installation
- name and signature of the installing person
- signature of the recipient
- registration number of the vehicle,
- data of the on-board unit

**Duration of processing:** for 8 years following the fulfilment of the order

**Recipients of the personal data:** The controller shall not provide the data obtained to third parties, with the exception of the processor(s) indicated in Section 7. The recorded data may be accessed only by the employees of the Controller and the designated employees of the processor(s).

**Possible consequences of the failure to provide the required data:** It is not possible to conclude a contract between the data subject and our Company, or install the product. The provision of the data is a prerequisite for fulfilment.

**Data subjects affected by the data processing:**

The partners involved (present) in the installation of the on-board unit performed by ITineris Kft. (or its contractor).

#### 4.9. Issuance of an invoice (in the case of a natural person data subject)

**Purpose of data processing:** issuing an invoice to the invoice payer, fulfilling legal requirements

**Legal ground of data processing:** according to legislation - Section 166 (1) of Act C of 2000

**Processed personal data:**

- Name of the invoice payer
- Billing address
- Invoice amount
- Purchased products, invoiced services

**Duration of processing:** until the deadline specified in the Accounting Act - Section 169 (2) of Act C of 2000

**Possible consequences of the failure to provide the required data:** The provision of data is mandatory.

**Recipients of the personal data:** The controller shall not provide the data obtained to third parties, with the exception of the processor(s) indicated in Section 7. The recorded data may be accessed only by the employees of the Controller and the designated employees of the processor(s).

**Data subjects affected by the data processing:**

The data subjects for whom the controller issues an invoice.

#### 4.10. Complaint handling, guarantee service

**Purpose of data processing:** Complaint investigation, performance, guarantee service in case of a complaint.

**Legal ground of data processing:** statutory obligation - Article 6 (1) c) of the GDPR, fulfilment of the obligations prescribed in the Consumer Protection Act and the Civil Code.

**Processed personal data:**

- name and signature of the complainant (in the case of paper-based notification)
- personal data provided during the complaint/notification

**Duration of processing:** Pursuant to the Consumer Protection Act, the Controller is obliged to keep the data and the related complaint letters for 5 years following the handling of the complaint.

**Recipients of the personal data:** The controller shall not provide the data obtained to third parties, with the exception of the processor(s) indicated in Section 7. The recorded data may be accessed only by the employees of the Controller and the designated employees of the processor(s).

**Possible consequences of the failure to provide the required data:** In case of missing the data, the data controller cannot process the complaints of the data subject, the provision of data is mandatory.

**Data subjects affected by the data processing:** The data subjects submitting a complaint to the controller.

#### 4.11. Call centre

**Purpose of data processing:** Enabling the User to communicate with the controller by telephone. Recording call centre conversations in case of communication, ordering and error and complaint notification.

**Legal ground of data processing:** voluntary consent of the data subject - Article 6 (1) a) of the GDPR, after the call is connected, the controller informs the data subject, the calling party, about the recording of the conversation, the availability of the privacy notice ([www.itineris.hu](http://www.itineris.hu)) and the data protection identification number of the call. If the caller does not disconnect the call, they give their voluntary consent to the call recording.

**Processed personal data:**

- name of the notifier
- personal data provided during the complaint/notification/conversation
- date and time of call
- phone number of the calling party

**Duration of processing:** The controller shall keep the data until the end of the year following the year of the call initiation or until the consent of the data subject is withdrawn

**Recipients of the personal data:** The controller shall not provide the data obtained to third parties, with the exception of the processor(s) indicated in Section 7. The recorded data may be accessed only by the employees of the Controller and the designated employees of the processor(s).

**Possible consequences of the failure to provide the required data:** If the data is not provided, the data controller will not be able to answer the telephone calls of the data subject.

**Data subjects affected by the data processing:** The data subject who make a telephone inquiry to the controller.

#### 4.12. Camera surveillance system

Cameras are in operation on the premises operated by the controller for the personal and property security of the data subjects and for other purposes.

The operation of these is advised to the data subjects with notification signs.

The activities related to the operation of the camera surveillance system are defined in the 'Electronic Surveillance System Data Processing Regulations' of the site, which is available at the site.

## 5. OTHER PROCESSING

Information on data processing not listed in this Notice will be provided when the data are recorded. We inform our clients that certain authorities, bodies performing public tasks, and courts may contact our company for the purpose of disclosing personal data. When the bodies specify the exact objective and the scope of data, our Company discloses personal data to the given body only to such an extent that is absolutely required for achieving the objective of the request, and if the execution of the request is required by law.

## 6. PERSONAL DATA TRANSFER TO A THIRD COUNTRY OR TO AN INTERNATIONAL ORGANISATION

Our company does not transfer Your personal data above to any third country or international organisation.

## 7. INFORMATION ON THE USE OF A PROCESSOR

During data processing, the controller transfers the data to the processor(s) contracted by them for the fulfilment of the contract.

**Recipient categories:** administrator service provider, server hosting, web hosting provider, sales/regional representative service providers, management system developer service provider,

The register containing the contact details of the processors is located at the company's headquarters.

## 8. CHILDREN

Our services are not intended for persons under the age of 16, and we ask that persons under the age of 16 do not provide personal data to the Controller.

If we become aware that we have collected personal data from a child under the age of 16, with the exception of the processing of data in accordance with legal regulations, we will take the necessary steps to erase the data as soon as possible.

## 9. AUTOMATIC DECISION-MAKING

Our company does not use automatic decision-making during its data processing procedures and data collection.

## 10. PERSONAL DATA STORAGE METHOD, SECURITY OF PROCESSING

The Company's IT systems and other data storage locations are located at the registered office and on the servers provided by the processor. Our Company selects and operates IT equipment used for processing personal data and providing services making sure that the processed data:

- a) are accessible by the authorised parties (availability);
- b) are authentic and genuine (authenticity of processing);
- c) remain certifiably unchanged (data integrity)
- d) are protected against unauthorised access (data confidentiality).

We pay particular attention to data security, take the technical and organisational measures and establish the procedural rules necessary to enforce the guarantees under the GDPR. We protect the data by means of suitable measures against unauthorised access, alteration, transfer, public disclosure, erasure or destruction as well as damage and accidental loss and ensures that stored data cannot be corrupted and rendered inaccessible due to any modification of the applied technique.

The information systems and networks of our Company and our partners are protected against computer supported fraud, as well as attacks by computer viruses, intrusion and service refusal. The operator also applies protection procedures at server and application level to guarantee security. Daily data backup is ensured. In order to avoid personal data breaches, our Company takes all possible measures, and in the event of such an incident - in accordance with our incident management policy - we take immediate action to minimise the risks and prevent any damage.

## 11. RIGHTS OF THE DATA SUBJECT, LEGAL REMEDY OPTIONS

The data subject may request information on the processing of their personal data, as well as request the rectification or erasure or revocation of their personal data, except for mandatory data processing, exercise their right to data portability and objection in the manner indicated at the time of data collection, at the above contact details of the Controller.

The rights and legal remedy options of the data subject under Act CXII of 2011 and Regulation (EU) No 2016/679 are defined below and are communicated to the data subjects.

The right to information, also known as the 'access rights' of the data subject: Pursuant to Act CXII of 2011 and Article 15 of Regulation (EU) No 2016/679, the Controller shall provide information at the request of the data subject

- on the data it processes and the categories of personal data,
- on the purpose of the data processing,
- on the legal ground of the data processing,
- on the duration of the data processing,
- in certain cases, on the retention period of the collected personal data or, if it is not possible, the aspects of determining such a retention period,
- in certain cases, if the personal data of the data subject are obtained from other sources, regarding any available information on the data source,
- in certain cases, on automated decision-making, including the profiling process, the logics applied in such processes and the significance of such data processing activities, as well as the expected consequences thereof for the data subject,
- of the data of the processor, if it employed a processor, and the circumstances, effects and measures taken to handle the personal data breach, and

- in the case of the transfer of the personal data of the data subject, the legal ground, purpose and recipient of the transfer.

The information is free of charge, provided that those requesting the information have not submitted any request for information for the same set of data in the current year to the Controller. Otherwise the refund of the costs can be claimed. Where any payment is made in connection with data that have been processed unlawfully, or the request led to rectification, the amount shall be refunded.

6. The Controller draws the attention of the data subjects to the fact that the information must be refused in accordance with Act CXII of 2011 a. if, pursuant to a provision of law, an international treaty or a binding legal act of the European Union, the Controller receives personal data in such a way that the transferring controller indicates, simultaneously with the transfer, the restriction of the data subject's rights provided for in the referenced law, or other restrictions on its processing.

b. in order to safeguard the external and internal security of the State, such as defence, national security, the prevention and prosecution of criminal offences, the safety of penal institutions, to protect the economic and financial interests of central and local government, safeguard the important economic and financial interests of the European Union, guard against disciplinary and ethical breaches in regulated professions, prevent and detect breaches of obligation related to labour law and occupational safety - including in all cases control and supervision - and to protect data subjects or the rights and freedoms of others.

The Controller is obliged to notify the National Authority for Data Protection and Freedom of Information of rejected requests for information annually by 31 January of the year following the relevant year.

Right to rectification: The Data Subject shall have the right to obtain from the Controller, without undue delay, the rectification of inaccurate personal data concerning them. Taking into account the purposes of the processing, the data subject has the right to have incomplete personal data completed, including by means of providing a supplementary statement. However, if the personal data does not correspond to reality and the personal data corresponding to reality is available to the Controller, the personal data must be corrected by the Controller, even without the request of the data subject.

Right to erasure, also known as the 'right to be forgotten': The data subject has the right to request the Controller to immediately erase their personal data and, upon receiving such a request, the Controller shall immediately erase the personal data of the data subject, if it is not precluded by mandatory data processing.

In addition to the above, the Controller is obliged to erase the data pursuant to Act CXII of 2011 and Regulation (EU) 2016/679 of the European Parliament and of the Council if

- the data processing is unlawful;
- the data is incomplete or inaccurate - and this condition cannot be legally remedied -, provided that the erasure is not precluded by law;
- the purpose of the data processing no longer exists or the legal time limit for retention has expired;
- so ordered by the court or by the Authority.
- the personal data requested to be erased are no longer needed for the purpose they were obtained for and managed in any way;
- the data subject objects to the processing, and there is no prevalent legitimate reason for the processing of the data;
- the personal data have to be erased for compliance with a legal obligation to which the Controller is subject;
- the personal data were collected in connection with the provision of information society services directly to children referred to in Article 8 (1) of Regulation (EU) No 2016/679.

If the Controller has made the personal data publicly available, and in the context of the above is required to erase it, they shall take the reasonable measures (including technical measures), taking into consideration the available technology and implementation costs, to ensure the other controllers processing the data are notified of the fact that the data subject has requested the erasure of the links to the personal data in question, together with any copy or duplicate of such personal data.

The Controller draws the attention of data subjects to the limitations of the right to erasure or 'right to be forgotten' arising from the EU Regulation, which are the following:

- a) exercising of the right to freedom of expression and information;
- b) compliance with a legal obligation which requires processing of personal data by Union or Member State law to which the controller is subject or performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- c) public interest that relates to public health
- d) public archiving, scientific and historical research or statistical use as per Article 89 (1) of Regulation (EU) No 2016/679, where the right of erasure would be likely to make it impossible or would seriously jeopardise such processing; or
- e) presentation, enforcement or defence of legal claims.

Right to restriction of processing, also known as 'right to blocking': The data subject has the right to have the Controller restrict the processing upon their request.

If there are reasonable grounds to believe that erasure could affect the legitimate interests of the data subject, the data shall be blocked. Blocked personal data shall be processed only as long as the processing purpose which prevented their erasure prevails.

If the data subject disputes the accuracy or validity of the personal data, but the validity or accuracy of the disputed personal data cannot be ascertained beyond doubt, the data shall be blocked. In that case the restriction relates to the period during which the Controller can verify the accuracy of the personal data;

Pursuant to the EU Regulation, the data shall be blocked, if

- a) the data processing activity has no legal ground, and the data subject does not consent to the erasure of the data but requests the restriction of their use;
- b) the Controller no longer needs the personal data for data processing purposes, but the data subject requests the data for the submission, enforcement or defence of legal claims; or
- c) the data subject objected to the data processing; in such cases the restriction shall only apply to the time period necessary to determine whether the Controller's justified needs precede the needs of the data subject.

Where processing has been restricted (blocked), such personal data shall, with the exception of retention, only be processed with the consent of the data subject or for the submission, enforcement or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the European Union or of a Member State.

The Controller hereby draws the attention of the data subjects to the fact that the data subject's right to rectification, erasure or blocking may be restricted by law to safeguard the external and internal security of the State, such as defence, national security, the prevention and prosecution of criminal offences, the safety of penal institutions, to protect the economic and financial interests of central and local government, safeguard the important economic and financial interests of the European Union, guard against disciplinary and ethical breaches in regulated professions, prevent and detect breaches of obligation related to labour law and occupational safety - including in all cases control and supervision - and to protect data subjects or the rights and freedoms of others.

The Controller shall, without undue delay and within a maximum of 30 days of receipt of the request, inform the data subject of the details of their request and/or rectify the data and/or erase and/or restrict (block) the data or take other action in accordance with the request, if no precluding reason prevails.

The Controller shall notify the data subject in writing of the rectification, erasure or restriction of the data processing, as well as all those to whom the data was previously transferred for the purpose of data processing. When requested by the data subject, the Controller shall inform the data subject of the recipients. Notification may be omitted if it does not harm the legitimate interests of the data subject with regard to the purpose of the processing, or if the information proves impossible or requires a disproportionate effort. The Controller is also obliged to notify the data subject in writing if the exercise of the data subject's rights cannot take place for any reason, and is obliged to indicate precisely the factual and legal reason and the legal remedies open to the data subject: the possibility of turning to the courts and the National Authority for Data Protection and Freedom of Information.

'Right to data portability': The data subject has the right to

- a) receive the personal data concerning them, which they have provided to a Controller, in a structured, commonly used and machine-readable format, and also has the right to
- b) transfer those data to another controller

without hindrance from the Controller to which the personal data have been provided if:

- a) the data processing is based on the provision of consent; and
- b) the processing activity is an automated process.

During the exercising of the right to data portability, the data subject has the right to request the direct transfer of the personal data between the controllers, if such a transfer is technically possible.

With regard to the data processing performed by the Controller, the conditions for the exercising of the right to data portability are not fulfilled (there is no automated data processing), therefore the data subject cannot exercise this right.

Right to objection: The data subject has the right to object to the processing of their personal data, including profiling, if:

- the processing (transfer) of the personal data is required only for the enforcement of the rights or legitimate interest of the Controller or the data recipient, with the exception of mandatory data processing;
- the use or transfer of personal data is done for direct business acquisition, public opinion polling or scientific research;
- the exercising of the right to objection is otherwise permitted by law.

The data subject may also object to processing for direct marketing purposes pursuant to Article 21 (3) of Regulation (EU) No 2016/679, after which the personal data shall no longer be processed for such purposes.

Where personal data are processed for scientific or historical research purposes or statistical purposes, the data subject, on grounds relating to their particular situation, shall have the right to object to the processing of personal data concerning them, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

The Controller - simultaneously with the suspension of the data processing - shall review the objection within the shortest possible time or within no more than 30 days following the submission of the request, and shall notify the requestor in writing of its decision. If the objection of the requestor is well-founded, the Controller shall terminate all processing operations (including data collection and transfer), block the data involved and notify all recipients to whom any of these personal data had previously been transferred concerning the objection and the ensuing measures, upon which these recipients shall also take measures regarding the enforcement of the objection.

Should the data subject disagree with the Controller's decision, or the Controller fails to comply with the referred deadline, they shall be entitled to initiate – within 30 days of receipt – a court action against it.

The data subject has the right to object to automated decision-making.

Judicial remedy: In the event of any infringement of their rights, the data subject may bring their case before the court. The court shall hear such cases in priority proceedings. The Controller must prove that the data processing complies with the provisions of the law.

In case of violation of your right to informational self-determination, you can make a notification or file a complaint:

National Authority for Data Protection and Freedom of Information  
Address: 1125 Budapest, Szilágyi Erzsébet fasor 22/c  
Phone: +36 (1) 391-1400, Fax: +36 (1) 391-1410  
www: <http://www.naih.hu>  
e-mail: [ugyfelszolgalat@naih.hu](mailto:ugyfelszolgalat@naih.hu)