

PRIVACY POLICY

(amended and restated)

Application of the Privacy Policy

Name of the organisation:	Hungarian Rail Association (HUNGRAIL)
Seat of organisation:	1066 Budapest, Teréz krt. 38.
Person in charge of the Policy:	Ilona Dávid, Chairperson
Date of entry into force of the Policy:	25 May 2018
Modified:	05 October 2018


This Policy lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules applicable to the free movement of personal data. The provisions of the Policy shall be applied during the specific data processing operations and when giving instructions and issuing information regulating data processing.

The data protection regulations applicable to the organisation's educational and training activities are set out in a separate appendix.¹

Scope of the Policy

This Policy is valid until revoked, its scope extends to all officers and employees of the organisation.

Date: 05 October 2018


..... Head
of the Organisation

Objective of the Policy

The purpose of the Policy is to harmonise the provisions of the organisation's other internal policies regarding data processing activities in order to protect the fundamental rights and freedoms of natural persons and to ensure the proper processing of personal data.

In the course of its activities, the organisation intends to fully comply with the legal requirements for the processing of personal data, in particular the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council, as well as the relevant Hungarian laws in force.

¹ September 2018

Another important goal of the Policy is to enable the employees of the organisation to lawfully process the data of natural persons by getting to know and complying with the Policy.

Basic terms and definitions

- **GDPR** (General Data Protection Regulation) means the new Data Protection Regulation of the European Union

Pursuant to the Act on Informational Self-determination and the Freedom of Information

'personal data' means any information relating to the data subject;

- **'special data' means any data belonging to the special category of personal data including data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation;**
- **'data subject' means any natural person who is or can be directly or indirectly identified on the basis of any information;**²
- **'controller'** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;
- **'processing'** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

'sub-processing' means all data processing operations by a data processor acting on behalf or under the instruction of the controller;³

² September 2018

³ September 2018

- **'third party'** means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;
- **'consent of the data subject'** means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signify their consent to the processing of personal data relating to them;⁴September 2018 **'restriction of processing'** means the marking of stored personal data with the aim of restricting their processing in the future;⁵
- **'pseudonymisation'** means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, as such additional information is kept by the Company separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person;
- **'filing system'** means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;
- **'data breach'** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised transmission or disclosure of, or unauthorised access to, personal data transmitted, stored or otherwise processed;⁶

Basic principles of data processing

Personal data must be processed lawfully, fairly and in a transparent and verifiable manner in relation to the data subject.

The collection of personal data is only permitted for specified, clear and legitimate purposes authorised by law or regulation or with the consent of the data subject, provided it is necessary for and proportionate to the performance of the controller's tasks set forth in the laws, protecting the legitimate interests of the data subject or other persons and eliminating or preventing any threat to the life, physical integrity or property of any person, or if the data subject has expressly disclosed the data concerned and it is necessary for and proportionate to achieving the purpose of the processing.⁷

⁴ September 2018

⁵ September 2018

⁶ September 2018

⁷ September 2018

The purpose of the processing of personal data must be appropriate and relevant and limited to the extent necessary.

The personal data collected must be accurate and kept up to date. Any inaccurate, erroneous, outdated or unneeded personal data must be deleted immediately and such deletion must be recorded.

Personal data must be stored in such a way that it should enable the identification of the data subject only for the necessary or prescribed time. Personal data may only be stored for a longer period if such storage is required by law, or for archiving in the public interest, or for scientific and historical research purposes or for statistical purposes.

Personal data must 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.⁸

The principles of data protection should apply to any information concerning any identified or identifiable natural person.

The employee/assistant of the organisation in charge of data processing is liable for the lawful processing of personal data under labour law, offence, and criminal law regulations. If the employee/assistant becomes aware that the personal data they process is inaccurate, incomplete or outdated, they must rectify the same or initiate such rectification by the employee responsible for recording the data.

Processing personal data

As natural persons may be associated with online identifiers provided by the devices, applications, devices and protocols they use, such as IP addresses and cookie IDs, therefore, when combined with other identifiers and information received by the servers, this data can be used to create a natural person's profile and identify the person concerned.

Processing is permitted only if the data subject gives their specific, informed and unambiguous consent to the processing of data by a clear affirmative act, such as by a written statement, including by electronic means, or an oral statement.

It shall also be deemed a consent to data processing if the data subject ticks the appropriate box when visiting the website. Silence, pre-ticked boxes or inactivity shall not be deemed as a consent.

⁸ September 2018

It shall also be deemed a consent if the user makes technical adjustments during the use of electronic services or makes a statement or takes action which clearly indicates the consent of the data subject to the processing of their personal data in that context.

Personal data concerning health includes all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject. This may include e.g.

- occupational health fitness data;
- registration for health services;
- the number, sign or data assigned to the natural person for the purpose of individual identification for health purposes;
- information about the data subject's illness, disability, disease risk, medical history, clinical treatment or physiological or biomedical condition, regardless of its source, such as a doctor or other healthcare professional, a hospital, a medical device or a diagnostic test.

Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or use of the personal data and/or the equipment used for the processing of the personal data.

Every reasonable step should be taken to ensure that any inaccurate personal data be rectified or deleted. Before starting the planned data processing, the data controller shall assess the effects of the planned data processing on the enforcement of the fundamental rights of the data subjects, taking into account its circumstances, in particular its purpose, the range of data subjects and the technology used in data processing operations.⁹

Lawfulness of data processing

Processing of personal data is lawful only if at least one of the following applies:

- the data subject has given their consent to the processing of their personal data for one or more specific purposes;
- processing is necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into a contract;

⁹ September 2018

- processing is necessary for compliance with a legal obligation to which the controller is subject;
- processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

According to the above, processing is deemed lawful where it is necessary in the context of a contract or an intention to enter into a contract.

Where processing is carried out in accordance with a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority, the processing should have a basis in Union or Member State law.

The processing of personal data should also be deemed lawful where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person. Processing of personal data based on the vital interest of another natural person should in principle take place only where the processing cannot be based on another legal basis.

Some types of personal data processing may serve both important grounds of public interest and the vital interests of the data subject, for instance when processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural or man-made disasters.

The legitimate interest of the controller, including the controller to whom the personal data may be disclosed, or of a third party may constitute a legal basis for the processing. Such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations where the data subject is a client or in the service of the controller.

The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned. The processing of personal data for direct marketing purposes may also be regarded as carried out for a legitimate interest.

In any case, the existence of a legitimate interest would need careful assessment including whether the data subject can reasonably expect at the time and in the context of the collection of the personal data that processing may take place for the given purpose.

The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data is processed in circumstances where data subjects do not reasonably expect further processing.

The data controller concerned has a legitimate interest in the processing of personal data by public authorities, IT emergency response units, network security incident management units, electronic communications network operators and service providers and security technology providers to the extent strictly necessary for and proportionate to ensuring network and IT security.

The processing of personal data for purposes other than those for which the personal data was initially collected should be allowed only where the processing is compatible with the purposes for which the personal data was initially collected. In such a case, no legal basis separate from that which allowed the collection of the personal data is required.

Moreover, the processing of personal data by official authorities for the purpose of achieving the aims, laid down by constitutional law or by international public law, of officially recognised religious associations, is carried out on grounds of public interest.

Data subject's consent, terms and conditions

- Where processing is based on consent, the Controller shall be able to demonstrate that the data subject has consented to the processing of their personal data.
- If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters.
- The data subject has the right to withdraw their consent at any time. The withdrawal of consent shall not affect the lawfulness of processing that was carried out based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.
- When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

The Controller **must not process** personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation, except where the data subject has given their express consent to the processing of the personal data concerned for one or more specific purposes.

The processing of personal data relating to decisions establishing criminal liability and criminal offenses and related security measures may only take place if it is carried out in the course of data processing by a public authority.

Data processing carried out by a data processor

A person or organisation may act as a data processor only if they provide adequate guarantees to implement technical and organisational measures to ensure the lawfulness of data processing and the protection of the rights of data subjects.

Such guarantees must be certified to the controller by the data processor before starting the data processing operation.

The data processor may use a sub-processor only if this is not prohibited by law, and if the data controller has given its prior ad hoc or general authorisation to use employ sub-processor in a public deed or in a private deed of full probative force.

Prior to any data transfer, the data controller or the data processor acting on their behalf or on their instruction shall check the accuracy, completeness and up-to-dateness of the personal data to be transferred.¹⁰

Sub-processors engaged by the company:

Company name	Registered office	Activity
Contirex Számviteli és Adószakértő Kft.	1026 Budapest, Nagyajtai u. 4/b.	accounting
		storage provider
SpedIT Informatikai Fejlesztő és Tanácsadó Korlátolt Felelősségű Társaság	1133 Budapest, Váci út 92.	IT
Kocsis és Papp Ügyvédi Iroda	1011 Budapest, Szilágyi Dezső tér 1.	legal activities

¹⁰ September 2018

The data processor shall keep a record of the data processing operations carried out by it on behalf or on the instruction of each data controller (hereinafter: register of data processors).

In the register of data processors, the data processor shall record:

- the names and contact details of the controller, the processor, the sub-processors and the processor's data protection officer;
- the types of data processing carried out on behalf or on the instruction of the data controller;
- in the case of international data transfer expressly requested by the controller, the fact of the international data transfer and the identification of the recipient third country or international organisation;
- a general description of the technical and organisational security measures implemented in accordance with the Act.

The register of controllers and processors shall be kept in written or electronic form and made available to the Authority upon request.¹¹

Processing which does not require identification

If the purposes for which the Controller processes personal data do not or no longer require the identification of a data subject by the Controller, the Controller shall not be obliged to retain any additional information.

Where the controller is able to demonstrate that it is not in a position to identify the data subject, the controller shall inform the data subject accordingly, if possible.

Notification of data subject, data subject's rights

The principles of fair and transparent processing require that the data subject be informed of the existence of the processing operation and its purposes **prior to the data processing**¹².

Where the personal data is collected from the data subject, the data subject should also be informed whether they are obliged to provide the personal data and of the consequences, where they do not provide such data. Such information may be provided in combination with standardised icons in order to give the data subject a meaningful overview of the intended processing in a transparent, intelligible and clearly legible manner.

¹¹ September 2018

¹² September 2018

Information related to the processing of personal data concerning the data subject must be provided to the data subject **in an easily accessible and readable form, with concise, clear and comprehensible content**¹³ at the time of data collection or, if data is collected from a source other than the data subject, within a reasonable time depending on the circumstances of the case.

Data subjects have the right of access to personal data which have been collected concerning them, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing. All data subjects should have the right to know, in particular, the purposes for which the personal data is processed and, where possible, the duration of the processing of personal data,

In particular, a data subject should have the right to have their personal data **rectified, supplemented or restricted**¹⁴¹⁵, erased and no longer processed where the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed, where a data subject has withdrawn their consent to the processing of personal data.

Where personal data is processed for direct marketing purposes, the data subject shall have the right to object, at any time and free of charge, to the processing of personal data concerning them for such purpose.

Review of personal data

In order to ensure that the personal data is not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review.

Period for regular review set by the head of the organisation: 1 year.

Responsibilities of the data processor

The controller shall apply appropriate internal data protection regulations in order to ensure lawful data processing. Such regulations shall cover the powers and responsibilities of the data controller.

It is the duty of the controller to implement technical and organisational measures adapted to all the circumstances of the data processing, in particular to its purpose and the risks of data processing threatening the fundamental rights of data subjects; ¹⁵ and to be able to demonstrate that the data processing activities comply with the legislation in force.

¹³ September 2018

¹⁴ September 2018

¹⁵September 2018

Those measures should take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons.

Taking into account the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures. Under this Policy, it shall review and, if necessary, update its other relevant internal regulations. When designing and implementing data protection measures, the controller shall take into account all circumstances of the data processing, in particular the state of the art of science and technology, the costs of implementing the measures, the nature, scope and purposes of the data processing, and the likelihood and severity of risks posed by the data processing to the enforcement of the data subjects' rights.¹⁶

The controller or processor shall keep adequate records of the data processing activities carried out under its authority, **data breaches and the data subject's right of access.**¹⁷ Each controller and processor must cooperate with the supervisory authority and make those records available to it on request, so that the authority can monitor those processing operations.

In the register of data controllers, the data controller must record

- **the data controller, including each and every joint controllers, and the name and contact details of the Data Protection Officer,**
- **the purpose or purposes of data processing,**
- **the recipients of data transmission including third-country recipients and international organisations to which the personal data processed is transmitted or planned to be transmitted,**
- **the range of data subjects and the data being processed,**
- **whether or not profiling is used,**
- **in the case of international data transfers, the range of the transferred data,**
- **the legal bases for data processing operations, including data transfers,**
- **where known, the date of deletion of personal data,**
- **a general description of the technical and organisational security measures implemented in accordance with the Act,**
- **the circumstances of any data breach occurring in relation to the data processed by it, the consequences of such breach and the action taken to address them,**
- **the legal and factual reasons for any measure restricting or denying the exercise of the data subject's right of access under the Act.**

The register of controllers and processors shall be kept in written or electronic form and made available to the Authority upon request.¹⁸

¹⁶ September 2018

¹⁷ September 2018

¹⁸ September 2018

Rights relating to data processing

Right to request information

Any person may request information through the provided contact details on what legal basis, for what data processing purpose, from what source and for how long their data is being processed by the organisation. Upon the data subject's request, information must be sent to the provided contact details without delay but no later than within 30 days.

Right to rectification

Any person may request through the provided contact details that their data be rectified. Upon such request, action must be taken and information must be sent to the provided contact details without delay, but no later than within 30 days.

Right to Erasure

Any person may request through the provided contact details that their data be erased. Such request must be satisfied without delay, but no later than within 30 days, and a notification must be sent to the provided contact details.

Right to blocking or restriction of processing

Any person may request through the provided contact details that their data be blocked. The blocking shall last as long as the indicated reason for blocking the data exists. Such request must be satisfied without delay but no later than within 30 days, and a notification must be sent to the provided contact details.

Right to object

Any person may object to the data processing through the provided contact details. The objection must be assessed within 15 days after its submission, and it must be decided whether the objection is founded, and the data subject must be notified of the decision by sending a notification to the provided contact details.

The data subject's remedies relating to data processing

National Authority for Data Protection and Freedom of Information

Mailing address: 1530 Budapest, Pf.: 5.

Address: 1125 Budapest, Szilágyi Erzsébet fasor 22/c

Phone: +36 (1) 391-1400

Fax: +36 (1) 391-1410

E-mail: [ugyfelszolgalat \(at\) naih.hu](mailto:ugyfelszolgalat@naih.hu)
URL <https://naih.hu>

In the event of any infringement of the data subject's rights, the recipient may turn to court against the controller. The court shall hear the case with priority. The data subject may choose to start the action at the court that has jurisdiction according to their place of residence or their place of stay.

Tasks of the organisation to ensure proper data protection

- * Privacy awareness. Professional qualifications must be ensured to comply with the law. It is essential that the employees are professionally trained and know the Policy.
- The purpose and criteria of data processing as well as the concept of personal data processing must be reviewed. The lawfulness of data management and data processing must be ensured in accordance with the Privacy Policy.
- The person affected by data processing must be properly notified. It should be noted that, if the processing is based on the data subject's consent, in case of doubt, the controller must prove that the data subject has consented to the processing.

The information provided to the data subject must be concise, easily accessible and easy to understand, and must therefore be worded and presented in a clear and comprehensible language.

- It is a prerequisite of transparent processing that the data subject be informed of the existence and the purposes of the data processing operation. The information must be provided before the data processing begins and the data subject has the right to information during the data processing until its termination.
- The main rights of the data subject are:
 - access to their personal data;
 - rectification of their personal data;
 - erasure of their personal data;
 - right to request restriction of the processing of their personal data;
 - objection to profiling and automated data processing;
 - right to data portability.
- The controller shall provide information to the data subject without undue delay and at the latest within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The obligation to provide information can be met by operating a secure online system through which the data subject can easily and quickly access the necessary information.

- The data processing operations of the organisation must be reviewed, and the right to informational self-determination must be ensured. The data subject's data must be erased without delay at their request if the data subject withdraws the consent on which the data processing is based.

It must be absolutely clear from the data subject's consent that they consent to the processing. If the processing is based on the data subject's consent, in case of doubt, the controller must prove that the data subject has consented to the data processing operation.

- In the case of processing the personal data of children, special attention must be paid to compliance with data processing rules. The processing of personal data relating to information society services offered directly to children is deemed lawful if the child has reached the age of 16. Where the child is below the age of 16 years, the processing of personal data is lawful only if and to the extent consent is given or authorised by the holder of parental responsibility over the child.

Any unlawful management or processing of personal data must be reported to the supervisory authority. In the case of a data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, report the data breach to the supervisory authority, unless the data breach is unlikely to result in a risk to the rights of the natural person concerned.

- In some cases, it may be appropriate for the controller to carry out a data protection impact assessment prior to the processing. The impact assessment should examine how the planned data processing operations affect the protection of personal data. If the data protection impact assessment finds that the processing is likely to involve a high risk, the controller must consult the supervisory authority before processing the personal data.
- A data protection officer must be appointed if the core activities consist of processing operations which, by virtue of their nature, their scope or their purposes, require regular and systematic monitoring of data subjects on a large scale. The purpose of the appointment of the data protection officer is to strengthen data security.

Data security

Data must be protected by means of appropriate measures particularly against unauthorised access, alteration, transmission, public disclosure, deletion or destruction, and accidental destruction and damage, and in addition, becoming inaccessible due to any changes in the applied technique.

For the purpose of the protection of databases which are stored electronically in different files, suitable technical solutions shall be introduced to prevent direct linking of data stored in these filing systems and the attachment of data to the persons concerned.

In determining and implementing the measures ensuring the security of processing, the current state of the art should be taken into account. Where there are alternative data processing solutions, the one selected shall ensure a higher level of protection of personal data, except if this would cause unreasonable hardship for the data controller.

Data breach

Data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

In the absence of appropriate and timely action, a data breach may cause physical, financial or non-financial damage to natural persons, including loss of control over, or restriction of, their personal data, discrimination, identity theft or misuse of identity.

Any data breach must be reported to the relevant supervisory authority without undue delay and not later than 72 hours after becoming aware of the same unless it can be proved in accordance with the principle of accountability that the data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

When the data breach is likely to result in a high risk to the rights and freedoms of natural persons, the data subject must be notified without undue delay so that they can take the necessary action.

Data processing for administrative and registration purposes

The organisation may also process personal data in cases related to its activities, as well as for administrative and registration purposes.

The processing is based on the informed, voluntary and express consent of the data subject. After detailed information – including on the purpose, legal basis and duration of the data processing, as well as the rights of the data subject – the data subject must be warned about the voluntary nature of the data processing. Consent to data processing must be recorded in writing.

Data processing for administrative and registration purposes may serve the following purposes:

- data processing of the members and employees of the organisation based on a legal obligation;
- data processing of persons in an agency relationship with the organisation for liaising, accounting and registration purposes;
- contact details of other organisations, institutions and businesses that have a business relationship with the organisation, which may include contact and identification information of natural persons.

The processing of data as described above is based on a legal obligation on the one hand and the data subject has consented to the processing of their data on the other hand (for example, registered on a website for an employment contract or as a partner, etc.)

In the case of documents sent to the organisation in writing, including personal data (such as CVs, job applications, other submissions, etc.), the data subject's consent is deemed to be given. Once the case is closed, the documents must be destroyed unless consent has been given for continued use. The fact of the destruction shall be recorded in writing.

In the case of data processing for administrative purposes, personal data will only be included in the case file and the records. The processing of such data lasts until the document on which the processing was based is discarded.

The processing of data for administrative and registration purposes shall be reviewed annually in order to ensure that the storage of personal data is limited to the time necessary, and any inaccurate personal data shall be erased without delay.

Compliance with the law must be ensured also in the case of data processing for administrative and registration purposes.

Data processing for other purposes

If the organisation wishes to carry out data processing that is not included in this Policy, the relevant internal policy must be supplemented first accordingly, or sub-policies corresponding to the new data processing purpose must be added.

Other documents related to the Policy

Documents and policies that contain, for example, a written statement of consent to data processing or, in the case of websites, describe the mandatory data processing information, should be linked to and managed together with the Privacy Policy.

Laws and regulations on which data processing is based

- REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (of 27 April 2016) on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
- Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information
- Act LXVI of 1995 on the Protection of Public Documents, Public Archives and Private Archive Materials.
- Government Decree No. 335/2005 (XII.29.) on the general requirements of document management at public administrative bodies.
- Act CVIII of 2001 on Certain Issues of Electronic Commerce Activities and Information Society Services
- Act C of 2003 on Electronic Communications