

DATA CONTROL AND DATA PROCESSING POLICY

1. Introduction

The **Lechner Knowledge Center Non-profit Ltd.** (hereinafter: Knowledge Center) controls personal data as authorized by law. The Knowledge Center performs data processing tasks as per law and contractual obligation. Considering that our IT system users are not to be expected to possess the exact information on whether the Knowledge Center manages their personal data as data controller or data processor, for a better understanding, this guide includes both our data control and data processing policy in a unified structure.

2. Data and contact information of the Knowledge Center

Head office and mailing address: 1111 Budapest, Budafoki út 59.

E-mail: info@lechnerkozpont.hu

Telephone: +36 (1) 279-2640, +36 (1) 279-2610

Company registration number: 01-09-996479

Tax number: 24225221-2-43

3. Definitions

| | |
|-----------------|---|
| data set | all data within the same register |
| data processing | the completion of technical tasks relating to data management operations, regardless of the method, tool or location of implementation as long as the technical task is carried out on data |
| data processor | a natural or legal person, or an organizational entity without legal personality carrying out data processing by contract – including contracts stipulated by law – signed with the data controller |
| data owner | the public service organization that produced or generated through its operation the data of public interest to be mandatorily disclosed electronically |

| | |
|---------------------|---|
| data control | regardless of the procedure applied, any operation or multiple operations carried out on data, especially the collection, recording, organization, storage, modification, utilization, query, transmission, disclosure, coordination, connection, restriction, erasure and destruction of data, as well as the prevention of further data use, the taking of photographs and making of audio and video recordings, the recording of physical attributes suitable for personal identification (e.g. finger or palm print, DNA sample, iris scan) |
| data controller | a natural or legal person, or an organizational entity without legal personality that defines – independently or in accordance with other parties – the purpose of and makes decisions regarding data control (including the applied tools), implementing or having their contracted data processor implement those |
| data identification | assigning a distinctive tag to data for the purpose of identification |
| data destruction | the complete physical destruction of media on which data is stored |
| data transmission | transferring data to a specified third person |
| data erasure | overwriting data in a way that makes it unrecoverable |
| data restriction | assigning a distinctive tag to data for the purpose of restricting – permanently or for a specified time – further handling of the data |
| EEA state | a member state of the European Union or another state applying the agreement on the European Economic Area, as well as a state in which citizens enjoy the same status as citizens of an EEA state according to an international treaty between the EU and its member states and the non-EEA member state |
| stakeholder | any specified natural person identified by personal data or identifiable either directly or indirectly |
| third party country | countries other than EEA states |
| third party person | a natural or legal person, or an organizational entity without legal personality other than the stakeholder, data controller or data processor |
| consent | the definitive and voluntary declaration of the will of the stakeholder, founded on adequate information and expressing unambiguous consent to the handling – either full-scale or covering only certain operations – of their personal data |

| | |
|------------------------------|---|
| open data for public benefit | other than data of public interest, any data the disclosure, knowability and availability of which is stipulated by law for public benefit |
| data of public interest | information and knowledge other than personal data, recorded in any form and manner, managed by and relating to the activities of or generated in relation to the tasks of an organization or person performing state or local governmental functions, or statutory public service, regardless of the manner of its management, its independent or collective nature, therefore especially concerning data pertaining to competence, jurisdiction, organizational structure, professional activity and the evaluation thereof, owned data types, legislation governing their operation, as well as data on management and contracts concluded |
| disclosure | making data publicly available |
| personal data | data related to the stakeholder – specifically their name, ID number, as well as one or more features describing their physical, physiological, mental, economic, cultural or social identity – and the conclusions drawn from those data |
| objection | a declaration of the stakeholder objecting against the handling of their personal data, requesting a cease to processing, along with the removal of those data |

4. Personal data management, data security

The Knowledge Center is committed to the protection of personal data. Within its own sphere of competence, the Knowledge Center takes the appropriate measures, develops the necessary procedures and establishes its internal regulations on data protection and data security in order for its personal data management to be in accordance with the Hungarian law and the relevant legal acts of the European Union, and thus earn the citizens' unwavering trust regarding the safety of their personal data.

Adhering to data security and data protection requirements in personal data management, the Knowledge Center acts in accordance with the provisions of **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)** (hereinafter: GDPR) and **Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information (hereinafter: Privacy Act)**, as well as relating data protection policies and legal practices, complying with the provisions of current legislation and taking into account major international recommendations on data protection.

With regard to the personal data in its possession, the Knowledge Center provides the necessary technical conditions and IT procedures that contribute to meeting data security standards and requirements without fail.

The Knowledge Center appointed a Data Protection Officer who possesses tertiary qualification, professional experience in the field of data protection, and IT skills. The Data Protection Officer is fully

entitled to oversee and take action in the processes of data control and data processing with regard to the personal data managed by the Knowledge Center in order to fully adhere to the requirements of the relevant Hungarian and EU legislation, the professional protocols, and the regulations of the Data Controller on data protection and security. The Knowledge Center – with the assistance of the Data Protection Officer – continuously updates its own regulations in order to conform to the legislative environment of personal data management, and as a reaction to technological change.

The Knowledge Center is responsible for keeping to data protection and data security requirements only relating to its data control and data processing activities that were assigned to it and defined as per law.

4.1. Scope of personal data, purpose, legal basis and duration of data control

4.1.1. Employee data

Not relevant for clients.

Regulated by the document titled “Information on processing the personal data of employees” available exclusively for the employees of the Knowledge Center.

4.1.2. Other personal data

Data control and processing may involve persons other than employees (security camera data, etc.).

4.1.2.1. Guest area – Contact data, guest register

The Knowledge Center is the data controller.

Purpose: guest identification and distinction from other guests/researchers in the Documentation Center, keeping in contact.

Legal basis: the consent of the stakeholder.

Scope of data: name, person visited, date and time, business, telephone number, licence plate number, and any other personal data disclosed by the stakeholder.

Deadline for deleting data: a year from recording.

Modification or removal of personal data may be requested

- by mail: 1111 Budapest, Budafoki út 59.
- by e-mail: info@lechnerkozpont.hu

4.1.2.2. Repository usage

The Knowledge Center is the data controller.

Purpose: keeping record of those who access repository data and use the copy service to ensure copyright protection.

Legal basis: the consent of the stakeholder and Act LXIII of 2012 on the Re-use of Public Sector Information, Section 10 (4).

Scope of data: registration date, name, address, telephone, e-mail.

Deadline for deleting data: 70 years after withdrawal of consent.

Modification or removal of personal data may be requested

- by mail: 1111 Budapest, Budafoki út 59.
- by e-mail: info@lechnerkozpont.hu

4.1.2.3. Registration to events

The Knowledge Center is the data controller.

Purpose: keeping record of event participants, sending invitations to similar events in the future.

Legal basis: the consent of the stakeholder.

Scope of data: name, e-mail, event registration, date of consent given, telephone (optional), organization and position.

Deadline for deleting data: upon withdrawal of consent.

Modification or removal of personal data may be requested

- by mail: 1111 Budapest, Budafoki út 59.
- by e-mail: info@lechnerkozpont.hu

4.1.2.4. Newsletters

The Knowledge Center is the data controller.

Purpose: sending e-mail newsletters to interested parties, providing current information and informing of changes.

Legal basis: the consent of the stakeholder and Act XLVIII of 2008 on the Basic Requirements of and Certain Restrictions on Commercial Advertising Activities, Section 6 (5).

Scope of data: name, e-mail, date.

Deadline for deleting data: withdrawal of consent, or 30 days for unconfirmed subscribers.

Modification or removal of personal data may be requested

- as stated in the newsletter, or
- by mail: 1111 Budapest, Budafoki út 59.
- by e-mail: info@lechnerkozpont.hu

4.1.2.5. Data stored in IT systems

4.1.2.5.1. TeIR user data

The Knowledge Center is the data processor.

Purpose: user identification, keeping in contact, sending e-mail newsletters to interested parties, providing current information and informing of changes.

Legal basis: the consent of the stakeholder and Act XLVIII of 2008 on the Basic Requirements of and Certain Restrictions on Commercial Advertising Activities, Section 6 (5).

Scope of data: name, e-mail, date, name and e-mail used for the customer portal, telephone.

Deadline for deleting data: upon withdrawal (cancelling registration).

Modification or removal of personal data may be requested

- online at www.teir.hu, under the tab 'Felhasználói adatok' (User data) (modification only), or
- by mail: 1111 Budapest, Budafoki út 59.
- by e-mail: teir@lechnerkozpont.hu

4.1.2.5.2. OÉNY sub-systems

The Knowledge Center is the data processor.

Purpose: the identification of users and other persons involved in construction.

For clients:

Legal basis: Act LXXVIII of 1997 on the Formation and Protection of the Built Environment, Section 58 (9), and Government Decree 313/2012. (XI.8.), Section 3 (1).

Scope of data:

- natural person identification data,
- home address, mailing address, head office,
- tax identification number, tax number,
- in the case of a legal person or organizational entity without legal personality, the name, tax identification number, and home address of the authorized representatives,
- title and document number of qualifications, registry number of eligibility to practice a profession,
- in case of electronic administration and contact, e-mail address, telephone number,
- fines, penalties, disciplinary measures.

In general, it is not possible to remove personal data. Modification may be requested

- through an electronic interface, under the corresponding tab, or
- by mail: 1111 Budapest, Budafoki út 59.
- by e-mail: info@lechnerkozpont.hu

For the personnel of authorities acting in official capacity:

Legal basis: personnel identification is a legitimate interest of the authority employing them, as well as of the OÉNY system operator.

Scope of data:

- data necessary for identification within the organization
name, position, workplace e-mail address, workplace telephone number

In general, it is not possible to remove personal data. Modification may be requested from the administrator of the authority.

For the personnel of public utility operating companies acting in such capacity:

Legal basis: personnel identification is a legitimate interest of the authority employing them, as well as of the OÉNY system operator.

Scope of data:

- data necessary for identification within the organization
name, position, workplace e-mail address, workplace telephone number, legal relationship

In general, it is not possible to remove personal data. Modification may be requested by the user personally, from the administrator of the public utility operating company.

Any other data control deadlines defined by legislation are indicated at the website of the given IT system.

4.1.2.5.3. E-TÉR sub-system

The Knowledge Center is the data processor.

Purpose: identifying users of different roles and assigning them to functions.

Legal basis: Section (1) e) of Article 6 of the GDPR, according to Section 16 (2) of Govt. Decree 218/2009. (X. 6.) (hereinafter: E-TÉR Decree) on the content requirements and detailed rules of aligning, drawing up, coordinating, accepting and publishing the regional development concept, the regional development programme, as well as the land use plan.

Scope of data:

for users having access to the system:

- natural personal identification data supplied by the stakeholder
- organization (hereinafter: Organization) the behalf on which the user acts (also supplied by the stakeholder)

Removal and modification of personal data may be requested from the Organization the behalf on which the user acts. Actual removal and modification of data is performed upon request from the Organization by Lechner Non-profit Ltd. as official administrator.

for data included in uploaded documents:

- data of the author of the plan: name, chamber membership, represented organization

Due to the nature of the uploaded documents, modification or removal of personal data is not possible.

In both cases, data may be stored indefinitely.

4.1.2.5.4. Smart city

The Knowledge Center is the data controller.

Purpose: when a third party submits an observation on a project, the Knowledge Center uses the provided e-mail address to contact the person who uploaded the project in question.

The legal basis of data control is the consent of the stakeholder, which may be withdrawn at any time. Should the stakeholder delete their personal data, the Knowledge Center has the right to restrict public access to the projects uploaded by the stakeholder in question.

Scope of data: mandatory: name, e-mail address

optional: name of organization

Deadline for deleting data: within 3 business days of the withdrawal of consent

Modification or removal of personal data may be requested

- by mail: 1111 Budapest, Budafoki út 59.
- by e-mail: okosvaros@lechnerkozpont.hu

4.1.2.5.5. European (Copernicus) land cover databases

The Knowledge Center is the data controller.

Purpose: informing users of changes and updates in the databases, making statistics of the fields of application of Copernicus data.

Legal basis: by filling in the questionnaire - which is not mandatory - consent is given to the control of personal data (GDPR Article 6, Section (1) a)).

Deadline for deleting data: upon withdrawal of consent.

Modification or removal of personal data may be requested

- by mail: 1111 Budapest, Budafoki út 59.
- by e-mail: info@lechnerkozpont.hu

4.1.2.5.6. GeoShop

The Knowledge Center is the data controller.

Purpose: providing the data service to the customer through the GeoShop system.

Including:

Purpose -1: registration, preparing orders, convenience functions.

Legal basis: the voluntary consent of the user by providing their personal data (GDPR Article 6, Section (1) a)).

Scope of data:

- name
- billing data
- billing address
- user IDs (including technical identifications)
- contact information (e-mail, telephone)
- language (Hungarian/English)
- favourite products

Deadline for deleting data: upon data modification by the user or withdrawal of consent.

Modification or removal of personal data may be requested

- at the geoshop.hu portal (<https://geoshop.hu/users/profile>)

Purpose -2: delivering the product to the customer.

Legal basis: performing product delivery (GDPR Article 6, Section (1) b)).

Scope of data:

- e-mail
- data of the ordered product, order placement date
- current billing data
- current billing address
- payment data, amount to be paid
- authorized user data

Deadline for deleting data: after billing, according to the Accounting Act of Hungary.

Modification or removal of personal data is not possible after order fulfilment.

4.1.2.6. Data control for direct marketing and research purposes

The Knowledge Center is the data controller.

The Data Controller may, with the voluntary consent of the stakeholder, use personal data for the following purposes:

- market research, opinion polling;
- client satisfaction surveys, improvement of services.

The condition of data use applicable to this section is the consent of the stakeholder, which should always be given voluntarily.

The stakeholder may, without explanation, withdraw their consent to the use of their personal data as described in this section.

The Data Controller shall each time inform contacted stakeholders of their right to withdraw consent.

4.1.2.7. Managing job applications

The Knowledge Center is the data controller.

Purpose: filling open positions at the Knowledge Center.

Legal basis: the consent of the stakeholder.

Scope of data: data necessary for the evaluation of job applications, such as

- name, date and place of birth, address, contact details,
- qualifications and previous work experience.

Deadline for deleting data: upon withdrawal of consent, otherwise 1 year.

Modification or removal of personal data may be requested

- as stated in the posted information, or
- by mail: 1111 Budapest, Budafoki út 59.
- by e-mail: hr@lechnerkozpont.hu

4.1.2.8. Training attendance data

The Knowledge Center is the data controller.

Purpose: verification of training attendance and justification of eligibility for the support granted.

Legal basis: the consent of the stakeholder.

Data transmission: data is transferred to the organization supporting the training.

Legal basis of data transmission: fulfilling contractual obligations.

Scope of data: attendance sheet of the training.

Deadline for deleting data: 5 years.

Due to the nature of data use and data transmission, modification or removal of personal data may be requested only during the training session.

4.1.2.9. Data control of university students doing an internship

The Knowledge Center is the data controller.

Purpose: completing the internship and informing the university thereof, concluding an employment contract with the student for the duration of the internship. See the details below.

Purpose -1: completing the internship.

Legal basis: pursuing the legitimate interest of the Knowledge Center (data saved for security purposes).

Scope of data: name, any internal IDs, other data necessary for employment (these are obtained directly from the student).

Deadline for deleting data: data are stored indefinitely.

Removal of personal data is not possible.

Modification or restriction of personal data may be requested, or objection against data control may be raised by the student

- by mail: 1111 Budapest, Budafoki út 59.
- by e-mail: hr@lechnerkozpont.hu
- during the internship only: by contacting the Data Protection Officer in person

Purpose -2: informing the university of completed internship.

Legal basis: legal obligation (according to the Higher Education Act of Hungary)

Scope of data: data required by the university - name, date of birth, student ID, data forwarded to the Knowledge Center by the university.

Deadline for deleting data: a year, but no more than two years after the termination of the contract with the university.

Removal or modification of personal data may be requested

- if the original data source is the university: from the university, which informs the Knowledge Center of any changes in the previously forwarded data.
- if the original data source is the student: at the contacts given for raising an objection.

Restriction of personal data may be requested, or objection against data control may be raised by the student

- by mail: 1111 Budapest, Budafoki út 59.
- by e-mail: hr@lechnerkozpont.hu
- during the internship only: by contacting the Data Protection Officer in person

Purpose -3: concluding an employment contract with the student for the duration of the internship.

Legal basis: legal obligation (according to the Labour Code of Hungary)

Scope of data: data defined by the Labour Code

- name, date and place of birth, address
- student ID, contact information
- tax identification number, social security number
- bank account number

Deadline for deleting data: 50 years.

Modification of personal data may be requested

- by mail: 1111 Budapest, Budafoki út 59.
- by e-mail: hr@lechnerkozpont.hu

4.1.2.10. Surveillance camera data

The Knowledge Center is the data controller.

Purpose: protecting the property and pursuing the legitimate interest of the Knowledge Center.

Legal basis: Act CXXXIII of 2005 on Security Services and the Activities of Private Investigators (Security Services Act).

Scope of data: camera images.

Deadline for deleting data: 3 days.

Due to the purpose of data control, modification or removal of personal data is not possible.

4.1.2.11. Access control system data

The Knowledge Center is the data controller.

Purpose: protection of the Knowledge Center's property.

Legal basis: the legitimate interest of the Knowledge Center.

Scope of data: name, access card ID, authorizations, traffic data (location, direction, time).

Deadline for deleting data: 30 days.

Due to the purpose of data control, modification or removal of personal data is not possible.

4.1.2.12. Contact person data of contractual partners

The Knowledge Center is the data controller.

Purpose: ensuring that the obtained information originates from the contractual partner.

Legal basis: the legitimate interest of the Knowledge Center.

Scope of data: name, contact information (e-mail, telephone), other data provided by the partner.

Data source: provided by the contractual partner, who is responsible for the lawful disclosure of the data.

Deadline for deleting data: same as the contract retention period.

Modification or removal of personal data may be requested from the contractual partner.

4.1.2.13. Contact person data of other (non-contractual) partners

The Knowledge Center is the data controller.

Purpose: ensuring that the obtained information originates from the partner.

Legal basis: the consent of the stakeholder.

Scope of data: name, contact information (e-mail, telephone), other data provided by the partner.

Data source: provided by the partner, who is responsible for the lawful disclosure of the data.

Deadline for deleting data: upon notification from the partner or withdrawal of consent.

Modification or removal of personal data may be requested from the partner.

4.2. Data security

The Knowledge Center ensures data security, taking the necessary technical and organizational measures with regard to data sets stored either on electronic or conventional, paper-based media, and developing the rules of procedure necessary for enforcing the applicable law, as well as data and privacy protection rules. As Data Processor, the Knowledge Center performs processes that are also in accordance with the requirements of the Data Controller.

Applying the appropriate measures, the Knowledge Center protects against unauthorized access, modification, transmission, disclosure, erasure or destruction, accidental destruction or damage of data, as well as from data becoming inaccessible due to the change of the technology applied. The Knowledge Center provides for the enforcement of data security rules through separate regulations, directives, and procedural orders. To guarantee the conditions of data security, the Knowledge Center ensures that all the employees involved are adequately trained.

In cooperation with the Data Processor, the Data Controller takes current technological development into consideration when defining and applying data security measures. The Data Controller chooses from multiple data control options the one that guarantees the highest level of personal data protection, unless it poses a disproportionate difficulty.

4.2.1. Protection of electronic records

The IT protection tasks of the Knowledge Center include taking care of

- measures guaranteeing protection against unauthorized access, including the protection of software and hardware tools, and physical protection (access protection, network protection);
- measures guaranteeing the recovery of data sets, including regular backups and the separate, secure handling of copies (data mirroring, data backup);
- the physical protection of data sets and data storage media, including protection against fire damage, water damage, lighting strike, or any other elemental damage, as well as ensuring the recovery of data damaged as a result of such an event (archiving, fire protection).

4.2.2. Protection of paper-based records

The Knowledge Center takes the necessary measures to ensure the protection of paper-based media, especially with regard to physical security and fire protection.

Employees and other persons acting on behalf of the Knowledge Center are obliged to keep the data storage media they use or have in their possession safe, regardless of how the data was recorded, and to protect the stored personal data against unauthorized access, modification, transmission, disclosure, erasure or destruction, as well as accidental destruction or damage.

4.3. Data transmission

Data transmission is typically performed with the consent of the stakeholder or with the authorization of the law. Any other legal basis concerning data transmission is indicated in the description of the given system.

The Data Controller provides regular data transmission to organizations as defined by law, the intervals and content of which is also defined by law.

In the case of statutory ad hoc data transmission, the legal basis of data control should always be confirmed. Should the legal basis be questionable, the assistance of a legal expert is required. Personal data may only be transmitted if its legal basis, purpose, and the person of the recipient are clearly defined. All instances of data transmission are to be documented in a way that proves their course and legality. This documentation consists mainly of properly issued documents requesting or approving data transmission.

The Data Controller is obliged to perform statutory data transmission.

In addition to the above, personal data may only be transmitted with the express consent of the stakeholder. If possible, a written consent should be obtained to later serve as proof. This may be omitted if the data transmission is of minor importance considering the recipient, purpose, or set of data. In the case of data transmission tied to stakeholder consent, the stakeholder shall be made aware of the recipient and purpose of data transmission before expressing their will.

The Data Controller keeps a log of data transmissions to make it possible to determine the recipient, legal basis and purpose of personal data transmission. The stakeholder may be granted access to the data transmission log, unless the provision of law prohibits them from being informed on the fact of data transmission.

4.4. Data processor

The Data Controller reserves the right to employ a data processor in its activities by permanent or ad hoc contract. Permanent data processing is primarily performed in administrative tasks relating to managing client relations and providing services, and the maintenance of IT systems. The employment of a data processor is governed by the applicable law, especially the provisions of the Privacy Act, and may only occur by written contract.

Upon request, the Data Controller informs the stakeholder on the person of the data processor and the details of their data processing activities, especially concerning the operations performed and the instructions received by the data processor.

The rights and obligations of the data processor regarding the processing of personal data are defined by the Data Controller within the constraints of the applicable law. The Data Controller is responsible for the legality of the instructions given for data management operations.

The data processor is responsible, within their scope of activities and the framework defined by the Data Controller, for the processing, modification, erasure, transmission and disclosure of personal data. The data processor may not employ another data processor when performing their activities.

The data processor may not make substantive decisions on data control, may only process obtained personal data in accordance with the instructions of the Data Controller, may not perform data processing for their own purposes, and is obliged to store and preserve personal data in accordance with the instructions of the Data Controller.

By providing guarantees in their terms and conditions, and taking the proper organizational and technological measures, the Data Controller ensures that stakeholder rights are not violated during the activities of the data processor, and that the data processor may only have access to their personal data if it is indispensable for performing their tasks.

4.5. Stakeholder rights

The stakeholder may ask information on the handling of their personal data, request the correction or – except in the case of mandatory data management – removal of their personal data as indicated at the time of recording, and by contacting the data controller via the provided contact information.

Upon the request of the stakeholder, the data controller gives information on the data managed by them or processed by their contracted data processor, the source thereof, the purpose, legal basis and duration of data control, the name, address and data management activities of the data processor, as well as the legal basis and recipient of any data transmission. The data controller provides a written statement of the requested information within no more than 30 days of submission. This information is free of charge if the stakeholder has not previously submitted any requests to the data controller pertaining to the same set of data in the current year. Otherwise, the data controller charges a fee.

The data controller shall perform the removal, restriction, or correction of personal data within 30 days. Should the data controller refuse to comply with the request of the stakeholder to remove, restrict or correct personal data, they shall inform the stakeholder of the grounds of their refusal within 30 days and in a written statement.

The stakeholder may object to the management of their personal data

- a) if personal data control or transmission only serves to fulfil the legal obligation of the data controller, or the legitimate interest pursued by the data controller, data receiver or a third party, except when data control is stipulated by law;
- b) if personal data control or transmission occurs for the purpose of direct marketing, conducting opinion polls or scientific research;
- c) in any other cases defined by law.

Within 15 days of the submission of the request, the data controller examines whether the objection is well-founded, and informs the stakeholder of their decision in a written statement. Should the data controller find the objection of the stakeholder well-founded, they cease control of – including further recording or transmission – and restrict personal data, informing previous recipients of that data about the objection and the resulting measures, who then shall proceed in a way that enforces the stakeholder's right to object.

Should the stakeholder disagree with the decision of the data controller, they may – within 30 days of disclosure – bring the case to court.

The data controller may not erase the stakeholder's personal data if data control is stipulated by law. However, personal data may not be transmitted to a recipient if the data controller agreed with the stakeholder's objection, or the court established the legitimacy of the protest.

Should the rights of the stakeholder be violated, they may file a case against the data controller, which shall be given priority by the court.

To seek legal remedy or file a complaint, please contact the Hungarian national authority for data protection and freedom of information.

Name: Nemzeti Adatvédelmi és Információszabadság Hatóság

Head office: 1125 Budapest, Szilágyi Erzsébet fasor 22/C.

Website: <http://www.naih.hu>

4.6. Data Protection Officer and data protection register

4.6.1. Data Protection Officer

With regard to its data control activities, the Knowledge Center appoints a Data Protection Officer, who assists in data control issues pertaining to the policy outlined here.

Stakeholders may seek the guidance of the Data Protection Officer concerning all data control issues covered by this policy.

The Data Protection Officer

- a) cooperates, assisting in decision-making concerning data control, as well as guaranteeing the rights of the stakeholders;
- b) oversees adherence to the provisions and data security requirements of the GDPR, the Privacy Act, and other legislation on data control, as well as the internal data protection and data security regulations;
- c) investigates received notifications, detects possible unauthorized data management and calls upon the data controller or data processor to cease such processes;
- d) contributes to the establishment of the internal data protection and data security regulations;
- e) keeps records for the internal data protection register;
- f) can be contacted at: adatvedelmi.felelos@lechnerkozpont.hu

4.6.2. Internal data protection register

The records in the internal data protection register are kept by the Data Protection Officer. In all instances of data control, the data protection register includes

- a) the purpose of data control,
- b) the legal basis of data control,
- c) the stakeholders,
- d) the description of data pertaining to the stakeholders,
- e) the source of data,
- f) the duration of data control,
- g) the kind and recipient of transmitted data, the legal basis of data transmission, including data transmission to third party countries,
- h) (in the case of a data processor other than the Knowledge Center) the name and address of the data processor, the location of actual data control and data processing, and the activities of the data processor relating to data control,
- i) the kind of data processing technology applied.

The purpose of the inner data protection register is to make it possible to determine the kind of data control the stakeholder may be the subject of, and the typical elements of that data control. Although the inner data protection register identifies data control processes, it shall not replace the detailed informing of the stakeholder.

The Data Protection Officer shall grant access to the inner data protection register to every stakeholder.