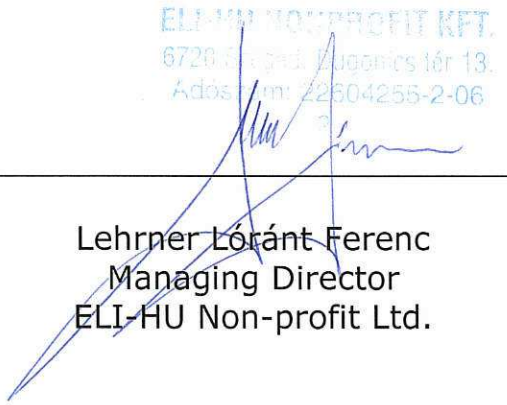
Instrucion's No. 8/2017. (05.12.) of

the Managing Director of

ELI-HU Non-profit Ltd's

Data Protection Regulation of ELI-HU Research and Development Non-profit Ltd.



Lehrner Lóránt Ferenc
Managing Director
ELI-HU Non-profit Ltd.

Data Protection Regulation of
ELI-HU Research and Development Non-profit Ltd.
2017

Company's name:	ELI-HU Research and Development Non-profit Ltd.
Address:	6720 Szeged Dugonics square 13.
Tax number:	22604255-2-06
Managing Director:	Lehrner Lóránt Ferenc
Entered into force with:	Instruction's No. 8/2017. (05.12.)
Effective as of:	12/05/2017.

ELI-HU
Research and Development
Non-profit Ltd.

Address: 6720 Szeged, 13 Dugonics Square

Phone number: (+36-1) 336-0542

e-mail: info@eli-alps.hu

website: www.eli-alps.hu

Data Protection Regulation

in effect from 12 May 2017

List of Contents

In order to register its internal data controlling processes and to guarantee the rights of the data subjects, ELI-HU Research and Development Non-profit Llc. (hereinafter the Company) creates the following Data Protection Regulation (hereinafter the Regulation).

Data controller

name:	ELI-HU Research and Development Non-profit Limited Liability Company
short name:	ELI-HU Non-profit Llc.
corporate registration number:	Cg.06-09-015211
headquarters:	6720 Szeged, 13 Dugonics Square
e-contact:	Info@eli-alps.hu
represented by:	Lóránt Ferenc Lehrner Managing Director

These present provisions should be interpreted in harmony with the provisions stipulated in the rest of the regulations of the Company. If regarding the protection of personal data there could be any contradiction between provisions stipulated herein and the provisions stipulated in any other regulations that already have been in force before this present regulation becomes effective, in such case the provisions of this present Regulation shall be of governing force.

Abbreviations used in this present Regulation:

Infotv.	Act XCII of 2011 on the Right of Informational Self-Determination and Freedom of Information
Mt.	Act I of 2012 on the Labour Code
Mvt.	Act XCIII of 1993 on Labour Safety
Ptk.	Act V of 2013 on the Civil Code
Sztv.	Act C of 2000 on accounting
Szvtv.	Act CXXXIII of 2005 on Security Services and the Activities of Private Investigators
NAIH or Authority	Hungarian National Authority for Data Protection and Freedom of Information

1. AIM AND SCOPE OF THIS REGULATION

By way of elaborating and publishing this present Regulation, the Company wishes to guarantee the rights of the data subjects for information as stipulated in Section 15 of Infotv.
The aim of this regulation is that the data subjects would get information concerning data controlled by the Company, including those processed by a data processor designated by the Company based on instructions given by the Company, also, concerning the sources from where they were obtained, the purpose, legal grounds and duration of processing, the name and address of any eventually engaged data processor and on its activities relating to data processing, and - if the personal data of the data subject is made available to others - the legal basis and the recipients.

By way of this present regulation, the Company wishes to guarantee the statutory order of the management of the records, the enforcement of the data protection principles and compliance with the requirements concerning data security as stipulated in the Constitution, furthermore the Company wishes to hinder unauthorised access to data as well as any unauthorised modification and/or publication of the data.

The scope of the Regulation covers all those procedures running at any of the Company's organisational units, in the course of which personal data as specified in Section 3, point 2 of Infotv. are processed.

The time scope of the Regulation is the period between 12 May 2017 and its withdrawal.

2. DEFINITIONS

The conceptual scheme applied by this present regulation is identical with the glossary given in Section 3 of Infotv., most specifically:

- ***Data subject:*** shall mean a natural person who has been identified by reference to specific personal data, or who can be identified, directly or indirectly
- ***Personal data:*** shall mean any information relating to the data subject, in particular by reference to his name, an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity, and any reference drawn from such information pertaining to the data subject;
- ***Sensitive data*** shall mean:
    - personal data revealing racial origin or nationality, political opinions and any affiliation with political parties, religious or philosophical beliefs or trade-union membership, and personal data concerning sex life,
    - personal data concerning health, pathological addictions, or criminal record;
- ***Personal data processed in criminal matters***: shall mean personal data that might be related to the data subject or that pertain to any prior criminal offense committed by the data subject and that is obtained by organizations authorized to conduct criminal proceedings or investigations or by penal institutions during or prior to criminal proceedings in connection with a crime or criminal proceedings;
- ***The data subject's consent:*** means any freely and expressly given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed without limitation or with regard to specific operations;
- ***The data subject's objection:*** shall mean an indication of his wishes by which the data subject objects to the processing of his personal data and requests that the processing of data relating to him be terminated and/or the processed data be deleted;
- ***Controller:*** shall mean the natural or legal person, or unincorporated body which alone or jointly with others determines the purposes of the processing of data, makes decisions regarding data processing (including the means) and implements such decisions itself or engages a data processor to execute them;
- ***Processing of data:*** shall mean any operation or set of operations that is performed upon data, whether or not by automatic means, such as in particular collection, recording, organization, storage, adaptation or alteration, use, retrieval, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction, and blocking them from further use, photographing, sound and video recording, and the recording of physical attributes for identification purposes (such as fingerprints and palm prints, DNA samples and retinal images);
- ***Disclosure by transmission/transfer:*** shall mean making data available to a specific third party;
- ***Public disclosure:*** shall mean making data available to the general public;
- ***Erasure of data***: shall mean the destruction or elimination of data sufficient to make them irretrievable;
- ***Blocking of data***: shall mean the marking of stored data with the aim of limiting their processing in future permanently or for a predetermined period;
- ***Referencing***: shall mean the marking of stored data for the purpose of identification;
- ***Destruction of data***: shall mean the complete physical destruction of the medium containing data;
- ***Data processing***: shall mean the technical operations involved in data control, irrespective of the method and instruments employed for such operations and the venue where it takes place, provided that such technical operations are carried out on the data;

- ***Data processor***: shall mean a natural or legal person or unincorporated organization that is engaged under contract in the processing of personal data, including when the contract is concluded by virtue of law;
- ***Data portfolio***: shall mean all data contained in a filing system;
- ***Third party***: shall mean any natural or legal person or unincorporated organization other than the data subject, the controller or the processor;
- ***EEA Member State***: shall mean any Member State of the European Union and any State that is a party to the Agreement on the European Economic Area, furthermore, any other country whose citizens are enjoying the same treatment as nationals of States who are parties to the Agreement on the European Economic Area by virtue of an agreement between the European Union and its Member States and a State that is not a party to the Agreement on the European Economic Area;
- ***Third country***: shall mean any State other than EEA Member States;
- ***Privacy incident/personal data breach***: shall mean the unlawful use or processing of personal data meaning, in particular, unauthorized access, alteration, transfer, disclosure by transmission or deletion as well as damage and accidental destruction.

If the glossary of terms described in the data protection legal rule currently in force (at the time of the creation of this present Regulation it is Infotv.) would alter from the glossary of terms described in this present Regulation, then the glossary of terms described in the legal rule shall be of governing force.

3. RULES OF DATA PROCESSING

In view of the fact that the right of informational self-determination is a fundamental right afforded by the Fundamental Law, in the course of any proceeding, the Company processes data only and exclusively on the basis of the provisions stipulated in the legal rules in force.

Personal data may exclusively be processed for a specific purpose to realize rights or fulfil obligations. The use of personal data in the control of the Company for private purposes is prohibited. Data controlling should always correspond with the purpose limitation principle.

Personal data may be processed by the Company to the minimum extent and for the shortest period necessary for the achievement of the specified and explicit purposes, where it is necessary for the implementation of certain rights and obligations. The purpose of processing must be satisfied in all stages of data processing operations, and in case the purpose of data processing has ceased or data controlling otherwise violates the law, data should be erased. Erasure of data is the responsibility of the employee of the Company who actually processes such data. Erasure could be checked by the person actually exercising employer's rights over the employee and by the internal data protection officer – provided that such officer has been appointed or designated by the Company. If such person has been designated or appointed, his/her name and contact data can be found in *Enclosure 1*.

The Company may process personal data only on the basis of the preliminary consent of the data subject – in the case of special/sensitive personal data on the basis of written preliminary consent – or on the basis of legal rule or statutory authorisation.

Prior to capturing a data, the Company in all cases informs the data subject about the purpose and the legal ground of data processing.

Employees actually processing data at the organisational units of the Company and the employees of organisations that are designated by the Company to participate in data processing or in any of the operations belonging to data processing are obliged to preserve personal data coming to their knowledge, as business secret. Persons processing and having access to personal data are obliged to make ***Declaration of Confidentiality*** *(Enclosure 3).*

If a person coming under the scope of this Regulation would gain knowledge of the fact that a personal data processed by the Company would be deficient, incomplete or outdated, he/she is obliged to rectify same or arrange for its rectification by the employee responsible for data capturing.

The Company makes the Senior Executive Officer or the internal Data Protection Officer – provided that such officer has been appointed or designated – responsible for managing a registry in order to check measures taken in respect of data protection incidents and in order to keep data subjects informed, which should contain the scope of personal data of the data subject, the scope and the headcount of data subjects concerned by a data protection incident, date, circumstances, impacts of the data protection incident and the measures taken in order to prevent incidents, furthermore other data specified in the legal rule requesting data processing (Enclosure 23/1). The Company informs the organisations and persons concerned by the data protection incident about the data protection incident occurred. Such organisations and persons are included in a list (Enclosure 23/2).

Data protection obligations applicable to natural or legal persons or organisations without legal personality that are designated by the Company to perform data processing activities should be enforced in the service contract concluded with the data processor. The Company concludes ***Data Processing Contract*** with the data processor as requested by Infotv. (Enclosure 24). Other issues to be included in such contract are regulated in Enclosure 17 of this present Regulation.

Photocopying personal identification cards

In due consideration of the position of NAIH, the Company does not make photocopies of personal identification cards. A photocopy of an authoritative deed is not suitable for identifying natural persons in view of the fact that the presence of the person is inevitable for identifying a person on the basis of an authoritative certificate. Obviously, a photo ID has probative force only in that case when on its basis the Company can ascertain that the person whose image is shown on the identification card and the person presenting such card are identical. A copy of an authoritative certificate has no probative force as regards the fact that it is a genuine copy of a valid authoritative certificate.

However, in order to preserve the principle of data capturing and data quality, the Company may make a masked photocopy (or scanned image – together: photocopy) about the authenticating certificate. In the course of photocopying, the Company will mask the identification card in such manner that only those parts will remain legible later that show data that the data subject is obliged to reveal. In such case the photocopy is created for data reconciliation. The company will immediately and irrevocably erase or destroy a photocopy when the data shown on the masked photocopy of such personal identification card have been collated with the completed job application form by the designated member of the HR staff but latest within 30 days from the creation of the photocopy.

4. DATA PROTECTION SYSTEM OF THE COMPANY

The ruling Senior Executive Officer of the Company will in due consideration of the specific features of the Company determine the data protection organisation and the scopes of responsibilities and authorities related to such activity, and designate a person who is responsible for supervising data processing.

Heads of all independent organisational units concerned will be responsible for the observation of the provisions stipulated in this regulation within their respective scopes of responsibilities.

In the course of their work, the members of the staff of the Company ensure that unauthorised persons would not view personal data and that personal data should be stored and located in such manner that they would not be accessible, readable, changeable and/or destroyable by unauthorised persons.

The data protection system of the Company should be supervised by the Senior Executive Officer through a data protection officer appointed or designated by him/her. The Company is not obliged by Section 24 of Infotv. or any other sectoral legal rule to designate or appoint an internal Data Protection Officer, however, in order to guarantee the rights of the data subjects on the possible highest level, the Senior Executive Officer may appoint or designate an internal Data Protection Officer. The name and the contact data of the internal Data Protection Officer can be found in *Enclosure 1*.

As regards data protection, the Senior Executive Officer:

a) is responsible for ensuring conditions necessary for exercising rights by the data subjects as specified in Infotv.;
b) is responsible for ensuring personal, material and technical conditions necessary for the protection of personal data processed by the Company;
c) is responsible for the elimination of any deficiencies or law violating circumstances occasionally discovered in the course of an inspection of data processing, and for initiating and/or pursuing a procedure necessary for the statement of personal responsibility;
d) supervises the activity of the internal Data Protection Officer;
e) may request inspection;
f) issues the Company's internal regulation regarding data protection.

Tasks of the internal Data Protection Officer related to data protection:

a) assists in ensuring the rights of data subjects;
b) initiates the procedure necessary for inclusion in the registry managed by the Hungarian National Authority for Data Protection and Freedom of Information (hereinafter NAIH);
c) by 15 January each year elaborates a report for the Senior Executive Officer regarding the execution of the Company's data protection tasks;
d) is entitled to inspect the observation of this present regulation at the organisational units;
e) keeps records of data transferring;
f) participates in the conference of internal Data Protection Officers organised by NAIH;
g) monitors changes in the legal rules related to data protection and freedom of information, and based on that, in justified cases, initiates the amendment of this present regulation;
h) participates in the elaboration of responses to queries received from NAIH by the Company as well as in the audit and/or data protection authoritative procedures initiated by NAIH;
i) requests general positions from NAIH if a data protection issue cannot unambiguously be answered on the basis of legal interpretation.

5. DATA SECURITY RULES

Physical protection

According to the information security regulation of the Company
In the interest of the security of personal data managed in hard copies, the Company applies the following measures:

- data may be known only by entitled persons, others may not have access to them, also, data may not be revealed for others;
- documents should be placed in a properly lockable, dry room, supplied with fire prevention and security devices;
- documents actually in the course of processing may be accessed by competent persons only;
- if the employee of the Company who is actually engaged in data processing would during the day wish to leave his/her room where data are processed, he/she should place data media in his/her care in a locked place, or should lock the office;

- after his/her work, the employee of the Company actually engaged in data processing should place paper-based data media in a locked place;
- if paper-based personal data would be digitised, the Company will apply security rules governing the storage of digital documents.

When the purpose of the processing of personal data stored on paper has been achieved, the Company takes measures in order to destroy the hard copies. In such case the Company designates an employee who will be responsible for such destruction. The employee responsible for destruction compiles a set of documents to be destroyed in cooperation with the organisational unit concerned about destruction. A three-strong destruction committee is obliged to take part in the destruction. The destruction should be recorded on a document attached as Enclosure 22 to this present regulation. The members of the committee verify whether or not those documents will be destroyed that have been recorded in the protocol attached herein as Enclosure 22.

If the media of the personal data is not paper but some other physical mean, the destruction of such physical mean shall be governed by the rules related to the destruction of papers.

Information technology protection

According to the information security rules of the Company
In the interest of the security of data stored on computers and/or on the network, the Company, in harmony with the prescriptions stipulated in the effective Information Security Manual for Users and the information security regulation, applies the following measures and guarantee elements:

- the computers used in the course of data processing either form the property of the Company or the Company is vested with rights amounting to ownership;
- data stored on computer could be accessed with valid, personalised and identifiable entitlements – at least user name and password – the company will arrange for changes of passwords regularly or in justified cases;
- any computer-aided operation with data is logged in a traceable manner;
- data stored on the network server (hereinafter the server) may be accessed by appropriately entitled and designated persons;
- when the purpose of the data controlling has been achieved, the deadline set for data processing has expired, then the file containing such data will irrevocably be deleted, such data could not be retrieved anymore;
- in the interest of the security of data stored on the network, in order to avoid loss of data, the Company arranges for backups and archiving on high-availability infrastructure;
- active data in databases containing personal data are backed up daily, such backup should cover the entire data portfolio of the central server and the media used in this procedure is magnetic data media;
- the magnetic data media containing data so backed up should be stored in an appropriately designed steel box at a fireproof place and manner;
- continuous protection against viruses is applied on the network handling personal data;
- the access to the network by unauthorised persons is blocked with available information technology devices and their application.

Server security

According to the information security rules of the Company
The flow of personal data controlled by the Company is achieved electronically with the help of servers, and their physical storage is achieved with the application of data storage devices. The data storage devices as well as the servers should be located in a room designed for this purpose. As regards this room, in accordance with the information security regulation, a staff should be designated whose members are permitted to access those devices and occasionally also the data stored on them. Entitlement for entering

the server room should be requested by the employee, and such request must be evaluated by the Head of IT (in cooperation with the internal Data Protection Officer if he/she has been designated or appointed).

Only those persons may enter this room who are defined and listed in Enclosure 20.

In the interest of the physical protection of servers installed in the server rooms, at the location where personal data are stored, the Company applies guarantee elements in accordance with the procedural rules of access eligibility management.

Access eligibility management

In accordance with the *Access eligibility management* procedure of the Company.

6. ENFORCEMENT OF THE RIGHTS OF DATA SUBJECTS

A data subject may request information about the processing of his/her personal data, furthermore he/she may request the rectification of his/her personal data or its erasure – except if data processing is regulated by legal rules – such requests should be addressed to the contact possibilities of the Company.

The Company is obliged to transfer such request or objection within three days from its receipt to the Head of the Organisational Unit that is vested with responsibility and authority regarding data processing.

The Head of the Organisational Unit vested with responsibility and authority should give a properly understandable answer to the request regarding the processing of the data of the data subject, latest within 25 – in the case when right to object was exercised within 15 – days in writing from the receipt of the request/objection.

Such notification should cover the information specified in Section 15 (1) of Infotv. if the notification of the person concerned may not be refused under the said Act.

The notification in general is free of charge, the Company charges reimbursable costs only in the case specified in Section 15 (5) of Infotv.

The Company refuses any application only for reasons specified in Sections 9 (1) or 19 of Infotv., which should be justified in accordance with Section 16 (2) of Infotv. in writing.

The Head of the Organisational Unit that processes data will rectify untrue data provided that the necessary data and the evidencing public deeds are available, furthermore, if causes specified in Section 17 (2) of Infotv. would prevail, he/she takes measures for the erasure of the processed personal data.

For the period necessary for the evaluation of the objection submitted by the data subject against the processing of his/her data – but at most for 5 days – the Head of the Organisational Unit responsible for data processing will suspend data processing, examine the groundedness of such objection, makes decision and notifies the applicant in accordance with Section 21 (2) of Infotv.

If the objection was justified, the Head of the Organisational Unit responsible for data processing will act in accordance with Section 21 (3) of Infotv.

In the event when a data subject exercises his/her rights but the case cannot be decided unambiguously, the Head of the Organisational Unit responsible for data processing may send the documents of the case together with his/her position related to the case to the internal Data Protection Officer and request his/her position, and the internal Data Protection Officer shall respond within three days.

The Company will reimburse any losses caused through unlawful processing of the data of a data subject or through breaching data security requirements, and/or will pay the restitution becoming due in the case when the data processor designated by the Company violated rights relating to personality. The Data Controller will be exempted from the liability for damages in respect of any losses and from the obligation to pay restitution if it can prove that such loss or the violation of the rights relating to personality of the data subject was caused by an inevitable cause outside the scope of data controlling. Similarly, the loss will not be reimbursed if it was a consequence of the deliberate and grossly negligent behaviour of the claimant.

The data subject may request legal remedy from or may submit his/her complaint to the Hungarian National Authority for Data Protection and Freedom of Information (1125 Budapest, Szilágyi Erzsébet fasor 22/C) or may turn to the court of justice competent in his/her place of residence or stay.

7. DATA PROCESSING PERFORMED BY AT THE COMPANY

Places of data processing:

Headquarters of the Company:
6720 Szeged, 13 Dugonics Square

Premises of the Company:
6720 Szeged, 85 Tisza Lajos boulevard
6728 Szeged, 5 Budapesti Street

Branch of the Company:
1027 Budapest, Residence II. Irodaház, 16 Ganz Street, 1st floor

Registration numbers of data processing procedures:
Apart from the exclusions stipulated in Section 65 (3) of Infotv., in accordance with Section 66 (1) of Infotv., the Company requested NAIH to include all of its data processing procedures into its registry. The identification numbers in the registry are listed in Enclosure 2 of this Regulation.

Data processing, data transfer:
The data processors involved in a given data processing as well as the addressees of data transfers are included in Enclosure 1 of this Regulation.

7.1. Data processing related to data of persons applying for job

Process of aspiring for a job with the Company

Interested persons can register via an online interface and can upload their resumes. For this purpose, the Company maintains an e-mail address (allas@eli-alps.hu), where resumes are received.

Selection of the appropriate employees is the responsibility of the back office, or in the case of engineer employees this responsibility is burdened on the HR partner and the professional manager, in the case of researchers this responsibility is burdened on three Senior Researchers and on the HR partner, thus in the course of performing tasks interrelated with data processing they are obliged to cooperate with the Company's co-worker responsible for data protection in order to guarantee the rights of the data subjects.

Common rules regarding "unsolicited resumes" and employee recruitment

In the case of resumes containing personal data sent in order to apply for a job (hereinafter: CV), the Company does not distinguish them according to the way of arrival: hard copy or digital CVs are evaluated in the same manner.

According to the general rule, the Company categorises resumes from the aspect of future utilisation – in view of positions becoming vacant or due for occupation later – and stores them in a digital database. Resumes so stored will be destroyed after one year in view of the fact that after the passing of such a period it can be presumed that the data are not of relevance any more from the aspect of job application.

In the case of any CV revealed for the Company, data processing is legally grounded by Section 6 (6) of Infotv. which says: "in other cases opened at the data subject's request, as regards the personal data he/she has supplied, the data subject's consent shall be deemed to have been granted".

Such supposedly granted consent given to data processing can be refuted, thus the data subject may withdraw his/her consent in accordance with this present regulation.

Special rules related to "unsolicited resumes"

In the case of application for an unadvertised position, the Company sends a response to the applicant, wherein information is given on the fact and the legal ground of data processing and the forms of objecting data controlling. The response titled "Response letter to resumes included in the database" is attached as Enclosure 4/1.

Special rules related to employee recruitment

According to the general rule, the Company stores CVs for later utilisation. The Company handles CVs and personal data included therein in accordance with the Regulation. The Company sends information in this respect – the text of this information is attached as Enclosure 4/1.

Special rules related to resumes received on the basis of recommendation

The Company is aware of and acknowledges the employee recommendation scheme. Any of the Company's employees may recommend his/her acquaintances in general or for a specific position – in such case the Company requests declaration from its employee (Enclosure 4/3) whether he/she is authorised by the subject of the data to reveal them for the Company. Such declaration will be kept until the deadline set for the storage of the given CV and will afterwards be destroyed together with the data contained in the CV.

However, in view of the fact that the Company just supposes the consent granted by the person concerned – the declaration made by the employee notwithstanding – therefore in all such cases an information letter is sent to the person recommended, wherein information is given concerning the fact and the legal ground of data processing and the forms of objecting data controlling. The response titled "Response letter to resumes received not from the person concerned" is attached as Enclosure 4/2 of this Regulation.

Data of the person concerned selected on the basis of their CV will further be processed (such as evaluation of competence) for the purpose of establishing employment relationship, therefore the rules of data processing as detailed in point 7.2 shall be applied.

purpose of data processing: selection of appropriate prospective employee for filling vacant positions and establishing employment relationship later
scope of processed data: name, date of birth, mother's name, residential address, qualification data, photo, other data given by the data subject, personal identification data of the recommender, completed successful background check
legal ground of data processing: consent of the data subject in accordance with sections 5 (1) a) and 6 (6) of Infotv.
time scope of data storage: one year from the inclusion of the date read on the recommender's declaration and in the resume
data storage method: electronically and in hard copy

7.2. Data processing related to employment relationship

The aim of the data processing related to employment relationship is the establishment, maintenance and termination of employment relationship.

Handling judicial records

In order to comply with the provisions stipulated in the legal rules and to meet commitments under other legal relationships, the Company reserves the right to hire employees who comply with its moral expectations, therefore the Company may make the employment conditional upon clean judicial records.

Clean judicial record will be checked by the HR partner who will verify the:

- validity (in a manner available for anyone), and
- content of the judicial record.

The Company may handle personal data processed in criminal matters only with the written consent of the data subject. The Company preliminarily notifies the data subject about the reason for handling personal data processed in criminal matters, which is making a decision about data subject's worthiness for the given position; therefore such data will be handled until this purpose would be achieved, until the passing of the decision.

The Company requests clean criminal record as a condition for filling a given specific job. In cases deserving special consideration, the Company's Senior Executive Officer, in the course of individual evaluation may make positive decision concerning worthiness for a given job if according to the judicial record:

- the nature and severity of the act committed is not irreconcilable with the expectations related to the job to be filled,
- court exoneration is in progress,
- statutory exoneration is opportune,
- there are other reasons deserving special consideration which guarantee that the Company's mission and principles would be not endangered.

In the course of aspiring for a job, data are transferred to the person vested with decision right on the ground discussed hereunder. The evaluation of the aptitude for the job is the responsibility of the back office whilst in the case of Engineers the responsibility is burdened on the Professional Managers and the HR partner. Data given in the course of application for a job could therefore be known not only by the Professional Managers and the HR Expert, but – in the special case described above – by the Senior Executive Officer of the Company, too.

The data may not be known by others than those indicated above, therefore other employees of the Company or any other person having legal relationship with the Company may not have access to such data in any manner or form.

In the course of the establishment of an employment relationship in respect of a given job, the data subject submits his/her valid judicial record. In view of the fact that the worthiness for the job is decided by the Professional Managers and the HR Expert, all of the data must be transferred to them. However, the Company in all cases seeks the best method for not restricting the privacy of the data subject and in consideration of the fact that a valid judicial record may within 90 days from its issue be used for purposes other than applying for a job with the Company, the Company physically does not file the judicial record of the data subject.

In order to achieve that data shown on the judicial record could be accessed only by the competent person, the Company obligatorily requests that in the course of the recruitment procedure the judicial record could be revealed by the applicant only for the Professional Managers and the HR Expert and – in the special case described in this present point – for the Company's Senior Executive Officer.

In the cases deserving special consideration, if in the course of the procedure aimed at the establishment of employment relationship, the data subject cannot present his/her judicial record, such judicial record may be mailed to the company in order to make documentation complete. In such case within a deadline of 30 days

- the Professional Manager makes decision on the employment relationship,
- the document will after the closure of the decision process be successively sent back to the data subject in a traceable manner.

In order that the Company could prove

- that in the course of the recruitment process, it has inspected the validity of the judicial record,
- what sort of available data were used for the evaluation of the prospective employee in the course of the recruitment process,

  together with the data necessary for the maintenance of the employment relationship, the following data will also be captured in the same manner and with the same storage deadline:
  - date of issue of the judicial record
  - deed number of the judicial record
  - identifier of the application for judicial record.

However, according to the legal rules these data do not qualify as special/sensitive personal data because they are not personal data processed in criminal matters. On the basis of the data mentioned above, the genuineness and the content of judicial records issued after 1 January 2013 can be successively verified in the system of KEKKH.

Therefore the Company does not store any judicial record either in the course of the recruitment procedure or during the employment relationship and does not make copy of the judicial record.

Photocopying of personal identification card

In due consideration of the position of NAIH, the Company makes masked photocopies of personal identification cards. A photocopy of an authoritative deed is not suitable for identifying natural persons in view of the fact that the presence of the person is inevitable for identifying him/her on the basis of such authoritative certificate. Obviously, a photo ID has probative force only in that case when on its basis the Company can ascertain that the person whose image is shown on the identification card and the person presenting such card are identical. A copy of an authoritative certificate has no probative force as regards the fact that it is a genuine copy of a valid authoritative certificate.

However, in order to observe principles related to data capturing and data quality, the Company may make a masked photocopy (or scanned image – together: photocopy) about the authenticating certificate of new recruits or employees modifying their data. In the course of photocopying, the Company will mask the identification card in such manner that only those parts will remain legible that the data subject is obliged to reveal in the course of joining the Company. In such case the photocopy is created for data reconciliation. The company will immediately and irrevocably erase or destroy a photocopy when the data shown on the masked photocopy of such personal identification card have been collated with the completed job application form by the designated member of the HR staff but latest within 30 days from the creation of the photocopy.

Processing health data related to medical fitness for work

Data related to the medical fitness of any of the data subjects will not be known and/or processed by the Company beyond the intended purpose. The company will pass its decision concerning the medical fitness of a given (prospective) employee for the work on the basis of the results of the relevant examination performed by the health care practitioner for the purpose of deciding fitness. The Company will process only those data that evidence medical fitness for work.
If in the course of the conclusion of employment contract it would be discovered that the given person is unfit for the job and therefore the employment relationship would not be established or would for this reason be terminated, the data processing deadlines and methods should be adjusted in parallel with that.

Disabled employees

From the aspect of data processing, identical rules are applicable for disabled workers than other employees of the Company, however, a larger scope of data are processed about them: see under *scope of data processed*. (The Company controls health data of disabled workers on the basis of the provisions stipulated by the law.)

Data processing related to maintenance and termination of employment relationship

The Company keeps labour records about its employees. Payroll accounting is performed by the Company.

The Company stores the data of employees electronically and in hard copy. Those personal data of employees will be captured that are necessary for establishing employment relationship. The Company captures data electronically in its database.

The legal ground of controlling employees' data is statutory authorisation (Act I of 2012 on the Labour Code, and the consent of the data subject (Section 5 (1) a) and 6 (6) of Infotv.).

Data processing in respect of travels organised during the existence of employment relationship

The Company keeps a travel registry that contains those personal data of its employees, which are inevitably necessary for the organisation of travels in the interest of performance of tasks related to employment relationship during the existence of their employment relationship.

The Company organises travels in accordance with Sections 31 and 32 of KBT, in the frames of centralised public procurement process through the portal operated by the Directorate-General for Public Procurement and Supply (KEF) (address: 1119 Budapest, Andor u. 47-49) (utaztatas.kef.gov.hu: Portal operator: 1122 Budapest, Acsády I. u. 13), and in accordance with Section 15 (2) of Government Decree 168/2004 (V.25.), and in the interest of its streamlined arrangement, the Company is obliged to satisfy by deadline its data delivery and other obligations related to the submission of demands and orders. KEF utilises the services provided by the following travel agencies:

OTP Travel Kft. (1051 Budapest, Nádor u. 21)
WECO Travel Kft. (1053 Budapest, Szép u. 2)
IBUSZ Utazási Irodák Kft. (Budapest, Dayka G. u. 3)

In the interest of complying with its data delivery obligation under the above legal rules and the streamlined arrangement of travels, the Company is obliged to furnish KEF with the following personal data regarding travellers: name, date of birth, citizenship, type, number, validity and the issuing authority of the personal identification card/passport.

Furthermore the Company, in the interest of the travellers, provides assistance in the arrangements for acquiring visa as necessary, and in this framework the co-workers dealing with travel organisation would contact the authorities or country representations issuing such visa in the interest of the persons concerned and transfer data for these organisations with the consent of the data subject.

The members of the staff engaged in travel organisation may process traveller-related actually valid digitised personal data that are necessary for travel arrangements within their scope of tasks exclusively in the interest of organising a travel, until the achievement of the aim of data processing but latest until the termination of the employment relationship. The members of the staff engaged in travel organisation are entitled to acquire traveller-related actually valid personal data from co-workers engaged in HR jobs, and such HR employees are entitled to furnish the members of the staff engaged in travel organisation with these data in the interest of measures to be taken for travel organisation.

The members of the Company's finance and controlling staff have access entitlement to the travel registry kept by the members of the staff engaged in travel organisation, exclusively until the compilation of the relevant accounts.

In the frames of travel organisation activities, the legal ground of data processing performed by the Company is statutory authorisation [Sections 31 and 32 of Kbt., and Sections 10 (1) and (2) of Mt.] and the consent of the data subject [Sections 5 (1) a) and 6 (6) of Infotv.].

Regarding the processing of data of employees, an information leaflet has been issued for the employees, which is attached as Enclosure 5/1 to this Regulation, whose aim is providing the employees with preliminary information on data processing.

Declarations concerning data processing related to employment relationship

If in the interest of the establishment, maintenance and termination of employment relationship and for evidencing the relevant entitlements and/or in recognition of obligations, declarations should be obtained from the employees, in the course of obtaining such declarations, the Company in all cases notifies the employee on the fact, legal ground and purpose of processing data revealed in such declarations.

If the validity of a declaration is conditional upon the presentation of a deed (personal identification card, student card), the company will not handle the data of such deed and/or its photocopied or scanned image in any manner, but will certify the presentation and the validity of such deed by virtue of the signature affixed by its appropriately entitled employee.

Employee training

The Company reserves the right to conclude contract with a third party for the training of its employees. If such training would be statutorily binding for the given job, then such third party processes data as the Company's designated data processor; in the case of any other sort of training, the transfer of a personal data to a third party is conditional upon the consent of the employee.

purpose of data processing: establishment, maintenance or termination of employment relationship, recognition of the relevant eligibilities and certifying obligations

scope of processed data:

- photo,
- identification number,
- name,
- name at birth,
- place and date of birth,
- citizenship,
- mother's name at birth,
- address of the place of residence,
- place of stay (if it differs from the place of residence),
- private pension fund
  - membership,
  - date of admission (day, month, year),
  - bank's name and code,
- tax identification mark,
- social insurance identification mark (TAJ number),
- pensioner registration number (in the case of retired employee),
- copy of the labour booklet (if any)
- declaration on debts,
- declaration on the observation of data security rules,
- current bank account number,
- starting date of employment relationship,
- type of insurance legal relationship,
- weekly working hours,
- telephone number,
- marital status,
- copy of the deed certifying qualification,
- certificate of medical fitness for work,
- job,
- medical fitness and necessity of eye-glasses,
- judicial record
  - date of issue,
  - registration number,
  - identifier of the application,
- after termination of the employment relationship, a certificate of the performance of closing medical examination of fitness for the job,
- expert resolution grounding disability status in the case of a disabled employee,
- in the case of work performed besides the main employment relationship
  - nature of the legal relationship,
  - name and headquarters of the employer,
  - monthly average work time at the workplace besides the main employment relationship,
  - activity to be performed,
- certificates related to the previous employment relationship:
  - certificate of the insurance legal relationship and regarding health insurance benefit
  - certificate of the employer on the termination of employment relationship
  - tax basis for 2015
- regarding additional vacation due under Section 120 of Mt.

- photocopy of the deed certifying the statement of disability in excess of fifty percent issued by the rehabilitation experts organisation
- photocopy of the deed certifying eligibility for disability subsidy,
- photocopy of the deed certifying eligibility for benefits of the blind.

In the case of disabled employees on the basis of Sections 21, 21/A and 21/B of Act CXCI of 2011 on the benefits due for disabled persons and the amendment of certain Acts, the above scope of data is supplemented as follows:

- documents containing data related to the health status that under Section 3, point 3 of Infotv. qualify as special/sensitive personal data:
  - opinion of the expert committee (ORSZI – National Office of Rehabilitation and Social Affairs),
  - resolution on disability.

legal ground of data processing: statutory authorisation under Sections 10 (1) and (3) of Act I of 2012 on Labour Code, and the consent of the data subject [Sections 5 (1) a) and 6 (6) of Infotv.]
time scope of data storage: until the achievement of the intended purpose of data processing, according to the general rule:

- related to the rights and obligations under employment relationship: until the termination of the employment relationship
- regarding eligibilities stemming from the employment relationship: until the deadline determined in the legal rules on the payment of pension benefits.

method of data processing: in hard copy and electronically

7.3. Processing data of relatives in connection with employment relationship

In order to guarantee certain benefits, the Company processes data of the employees' relatives in connection with employment relationship. Data of third parties so obtained could be captured and processed not in excess of the necessary data content.

Such benefits can be the following: additional vacation, utilisation of family tax benefit, applying for subsidised travel pass qualifying as non-taxable in-kind benefit, and non-taxable school starting subsidy.

In the case when the employee submits the data of a third person, the employee is obliged to obtain the consent of such third person in order that the Company can certify that it is authorised to control the data of a third party. Such declaration is attached as Enclosure 6 to this Regulation.

purpose of data processing: to guarantee benefits in connection with employment relationship
scope of processed data: name, name at birth, place and date of birth, citizenship, mother's name at birth, residential address, tax identifier, TAJ number and contact data of the close relative of the employee
legal ground of data processing: consent of the data subject [Section 5 (1) a) of Infotv.]
time scope of data storage: until the achievement of the intended purpose of data processing, according to the general rule:

- related to the rights and obligations under employment relationship: until the termination of the employment relationship
- regarding eligibilities stemming from employment relationship: until the deadline determined in the legal rules on the payment of pension benefits

method of data processing: in hard copy and electronically

7.4. Data processing in connection with other form of employment legal relationship

The Company employs persons under other form of employment legal relationship.

Publication of scientific materials created by researchers is regulated in a separate regulation.

Handling judicial records

In order to comply with the provisions stipulated in the legal rules and meet commitments under other legal relationships, the Company reserves the right to hire employees who comply with its moral expectations, therefore the Company may make the employment conditional upon clean judicial records.

Clean judicial record will be checked by the HR partner who will verify the:

- validity, and
- content of the judicial record.

The Company may handle personal data processed in criminal matters only with the written consent of the data subject. The Company preliminarily notifies the data subject about the reason for handling personal data processed in criminal matters, which is making a decision about data subject's worthiness for the given position; therefore such data will be handled until this purpose would be achieved, until the passing of the decision.

The Company requests clean criminal record as a condition for filling a given specific job. In cases deserving special consideration, the Company's Senior Executive Officer, in the course of individual evaluation may make positive decision concerning worthiness for a given job if according to the judicial record:

- the nature and severity of the act committed is not irreconcilable with the expectations related to the job to be filled,
- court exoneration is in progress,
- statutory exoneration is opportune,
- there are other reasons deserving special consideration which guarantee that the Company's mission and principles would be not endangered.

In the course of aspiring for a job, data are transferred to the person vested with decision right on the ground discussed hereunder. The evaluation of the aptitude for the job in the case of researchers is the responsibility of 3 expert researchers and the HR expert. Data given in the course of application for a job could therefore be known not only by 3 expert researchers and the HR Expert, but – in the special case described above – by the Senior Executive Officer of the Company, too.

The data may not be known by others than those indicated above, therefore other employees of the Company or any other person having legal relationship with the Company may not have access to such data in any manner or form.

In the course of the establishment of other form of employment legal relationship in respect of a given job, the data subject submits his/her valid judicial record. In view of the fact that the worthiness for the job is decided by the 3 responsible researchers and the HR Expert, all of the data must be transferred to them. However, the Company in all cases seeks the best method for not restricting the privacy of the data subject and in consideration of the fact that a valid judicial record may within 90 days from its issue be used for purposes other than applying for a job with the Company, the Company physically does not file the judicial record of the data subject.

In order to achieve that data shown on the judicial record could be accessed only by the competent person, the Company obligatorily requests that in the course of the recruitment procedure the judicial

record could be revealed by the applicant only for the 3 responsible researchers and the HR Expert and – in the special case described in this present point – for the Company's Senior Executive Officer.

In the cases deserving special consideration, if in the course of the procedure aimed at the establishment of other form of employment legal relationship, the data subject cannot present his/her judicial record, such judicial record may be mailed to the company in order to make documentation complete. In such case within a deadline of 30 days

- the Professional Manager makes decision on the other form employment legal relationship
- the document will after the closure of the decision process be successively sent back to the data subject in a traceable manner.

In order that the Company could prove

- that a in the course of the recruitment process, it has inspected the validity of the judicial record,
- what sort of available data were used for the evaluation of the prospective employee in the course of the recruitment process,

  together with the data necessary for the maintenance of the employment relationship, the following data will also be captured in the same manner and with the same storage deadline:
  - date of issue of the judicial record
  - deed number of the judicial record
  - identifier of the application for judicial record.

However, according to the legal rules these data do not qualify as special/sensitive personal data because they are not personal data processed in criminal matters. On the basis of the data mentioned above, the genuineness and the content of judicial records issued after 1 January 2013 can be successively verified in the system of KEKKH.

Therefore the Company does not store any judicial record either in the course of the recruitment procedure or during the employment relationship and does not make copy of the judicial record.

Photocopying of personal identification cards

In due consideration of the position of NAIH, the Company does not make photocopies of personal identification cards. A photocopy of an authoritative deed is not suitable for identifying natural persons in view of the fact that the presence of the person is inevitable for identifying him/her on the basis of such authoritative certificate. Obviously, a photo ID has probative force only in that case when on its basis the Company can ascertain that the person whose image is shown on the identification card and the person presenting such card are identical. A copy of an authoritative certificate has no probative force as regards the fact that it is a genuine copy of a valid authoritative certificate.

However, in order to observe principles related to data capturing and data quality, the Company may make a masked photocopy (or scanned image – together: photocopy) about the authenticating certificate of new recruits or employees modifying their data. In the course of photocopying, the Company will mask the identification card in such manner that only those parts will remain legible that the data subject is obliged to reveal in the course of joining the Company. In such case the photocopy is created for data reconciliation. The company will immediately and irrevocably erase or destroy a photocopy when the data shown on the masked photocopy of such personal identification card have been collated with the completed job application form by the designated member of the HR staff but latest within 30 days from the creation of the photocopy.

Processing health data related to medical fitness for work

Data related to the medical fitness of any of the data subjects will not be known and/or processed by the Company beyond the intended purpose. The company will pass its decision whether or not a given

(prospective) employee to be employed under other form of employment relationship would be fit for the work, on the basis of the results of the relevant examination performed by the health care practitioner for the purpose of deciding fitness. The Company will process only those data that evidence medical fitness for work.
If in the course of the conclusion of employment contract it would be discovered that the given person is unfit for the job and therefore such other legal employment relationship would not be established or would for this reason be terminated, the data processing deadlines and methods should be adjusted in parallel with that.

As regards the processing of personal data of persons employed under other form of employment legal relationship (researchers), an information material has been elaborated with the aim of providing the data subjects with preliminary information on data processing, which is attached as Enclosure 5/2 to this regulation.

Data processing in respect of travel organisation

The Company keeps a travel registry containing those personal data of persons employed under other form of employment legal relationship, which are inevitably necessary for the organisation of travels in the interest of performance of tasks related to their legal relationship.

The Company organises travels in accordance with Sections 31 and 32 of KBT, in the frames of centralised public procurement process through the portal operated by the Directorate-General for Public Procurement and Supply (KEF) (address: 1119 Budapest, Andor u. 47-49) (utaztatas.kef.gov.hu: Portal operator: 1122 Budapest, Acsády I. u. 13), and in accordance with Section 15 (2) of Government Decree 168/2004 (V.25.), and in the interest of its streamlined arrangement, the Company is obliged to satisfy by deadline its data delivery and other obligations related to the submission of demands and orders. KEF utilises the services provided by the following travel agencies:
OTP Travel Kft. (1051 Budapest, Nádor u. 21.)
WECO Travel Kft. (1053 Budapest, Szép u. 2.)
IBUSZ Utazási Irodák Kft. (Budapest, Dayka G. u. 3.)

In the interest of complying with its data delivery obligation under the above legal rules and the streamlined arrangement of travels, the Company is obliged to furnish KEF with the following personal data regarding travellers: name, date of birth, citizenship, type, number, validity and the issuing authority of the personal identification card/passport.
Furthermore the Company, in the interest of the travellers, provides assistance in the arrangements for acquiring visa as necessary, and in this framework the co-workers dealing with travel organisation would contact the authorities or country representations issuing such visa in the interest of the persons concerned and transfer data for these organisations with the consent of the data subject.

The members of the staff engaged in travel organisation may process traveller-related actually valid digitised personal data that are necessary for travel arrangements within their scope of tasks exclusively in the interest of organising a travel, until the achievement of the aim of data processing but latest until the termination of the employment relationship. The members of the staff engaged in travel organisation are entitled to acquire traveller-related actually valid personal data from co-workers engaged in HR jobs, and such HR employees are entitled to furnish the members of the staff engaged in travel organisation with these data in the interest of measures to be taken for travel organisation.

In the frames of travel organisation activities, the legal ground of data processing performed by the Company is statutory authorisation [Sections 31 and 32 of Kbt.], and the consent of the data subject [Sections 5 (1) a) and 6 (6) of Infotv.]

purpose of data processing: establishment or termination of employment under other employment legal relationship, recognition of the related eligibilities and certification of obligations

scope of processed data: the data subject's

- photo,
- identification number,
- name,
- name at birth,
- place and date of birth,
- citizenship,
- mother's name at birth,
- address of the place of residence,
- place of stay (if it differs from the place of residence),
- tax identification mark,
- tax number
- social insurance identification mark (TAJ number),
- current account number,
- starting date of the employment under other employment relationship,
- telephone number,
- job,
- medical fitness and necessity of eye-glasses,
- judicial record
  - date of issue,
  - registration number,
  - identifier of the application,

legal ground of data processing: consent of the data subject [Sections 5 (1) a) and 6 (6) of Infotv.]

time scope of data storage: until the achievement of the intended purpose of data processing, according to the general rule:

- related to the rights and obligations of persons employed under any other form of employment legal relationship: until the termination of the legal relationship,
- regarding eligibilities stemming from other form of employment legal relationship: until the deadline determined in the legal rules on the payment of pension benefits.

method of data processing: in hard copies and electronically

7.5. Data processing in connection with the surveillance of the technical devices of employees

The employer may supervise the employees as regards their behaviour conducted in the context of the employment relationship. Such surveillance is legally grounded by Sections 11 (1) and (2) of Mt.

The Company notifies the employees in advance on the application of technical devices that serve for the surveillance of the employees.

In justified cases the Company furnishes employees with computer, company telephone, e-mail address and internet access for personal use. The Company informs employees on the rules of usage and the possibility of surveillance in a document titled ***Information Security Manual for Users***.

purpose of data processing: in accordance with the lawful business interests of the Company, surveillance of employees under Section 11 (1) of Mt., specifically surveillance of the usage of computer, e-mail address, company telephone and internet access in the personal use of employees.
scope of processed data: personal data captured in the course of surveillance, specifically private e-mail addresses, private telephone numbers, photographs, personal computer documents, internet browsing history, cookies, the fact of perceiving any misdemeanour in the frames of employment relationship, description of the misdemeanour.
legal ground of data processing: Section 11 (1) of Act I of 2012 and occasionally Section 5 (1) a) of Act CXII of 2011.
time scope of data storage: one year from the surveillance, but latest the lapse of any demand stemming from the surveillance.
data storage method: electronically

7.6. Data processing in connection with the surveillance of the technical devices of persons employed under other form of employment legal relationship

The Company may supervise data subjects as regards their behaviour conducted in the frames of their other employment legal relationship. Such surveillance is legally grounded by Sections 11 (1) and (2) of Mt.

Persons employed under other form of employment legal relationship are notified by the Company in advance on the application of technical devices that serve for the surveillance of the employees.

The Company furnishes persons employed under other forms of employment legal relationship with computer, company telephone, e-mail address and internet access for personal use. The Company informs data subjects on the rules of usage and the possibility of surveillance in a document titled Information Security Manual for Users.

purpose of data processing: in accordance with the lawful business interests of the Company, surveillance of persons employed under any other form of employment relationship, in accordance with Section 11 (1) of Mt., specifically surveillance of the usage of computer, e-mail address, company telephone and internet access in the personal use of persons employed under any other form of employment relationship.
scope of processed data: personal data captured in the course of surveillance, specifically private e-mail addresses, private telephone numbers, photographs, personal computer documents, internet browsing history, cookies, the fact of perceiving any misdemeanour in the frames of employment relationship, description of the misdemeanour.
legal ground of data processing: Section 11 (1) of Act I of 2012 and occasionally Section 5 (1) a) of Act CXII of 2011
time scope of data storage: one year from the surveillance, but latest the lapse of any demand stemming from the surveillance
data storage method: electronically

7.7. Surveillance of fitness for work from the labour safety aspect

Section 52 (1) a) of Mt. states that employees and persons employed under any other form of employment legal relationship are obliged to appear at the place and time specified by the employer in a condition fit for work.

On the basis of the authorisation ensured in Section 2 (3) of Mvt., as regards impairment by alcohol, the employer determines the requirements concerning health safe and secure work practices as follows:

In accordance with Section 60 (1) of Mvt. employees and persons employed under any other form of employment legal relationship may perform work in a condition fit for the work, in due consideration of the rules and instructions related to labour safety, and in accordance with the labour safety training. The employee is obliged to cooperate with his/her colleagues and perform his/her work in such manner that therefore his/her own or anybody else's health or corporeal integrity would not be endangered.

In respect of each and every job the Company prohibits its employees and other persons employed under any other form of employment legal relationship from being present at the work premises under alcoholic influence – this should be applicable to those cases when the person concerned stays in the premises out of his/her working hours before/after working, in view of the fact that a person impaired by alcohol could endanger the safe work of others. It is prohibited to enter the premises of the company or the company's work premises elsewhere, under the influence of alcohol, consume alcohol there, perform work under the influence of alcohol.

Exemption from this rule can be granted by the Senior Executive Officer in writing.

The conditions of secure work practices are endangered by unfitness for work, for instance impairment by alcohol. Therefore the persons concerned must be in a condition fit for work not only when appearing on the work premises but fitness for work must be maintained until the end of the work time.

In the course of performing work, employees and persons employed under any other form of employment legal relationship may not endanger their own or anybody else's health or corporeal integrity.

By virtue of its obligation to arrange for the secure conditions of work practices, the Company is obliged to ascertain that employees and persons employed under any other form of employment legal relationship observe the relevant prescriptions. Rules related to the surveillance of the observation of labour law prescriptions are described in more detail in Mt. as well as in Mvt.

Section 54 (7) b) of Mvt.: In the interest of occupational safety and health, employers shall observe the following general requirements: routinely review work conditions and ensure that they conform with requirements, and the workers and other persons employed in legal work performance relationship have knowledge of and observe the provisions pertaining to them.

Surveillance of the observation of labour safety rules is the responsibility of the Company's Labour Safety Officer who could be appointed by the Senior Executive Officer of the Company in accordance with Section 57 (1) of Mvt. If he/she would be prevented from acting, the Labour Safety Officer may delegate the scope of surveillance authority to the security guards employed by the designated security services in accordance with Szvtv. Testing at the gatekeeper service may be performed exclusively by the members of the security staff.

However, testing of alcoholic impairment as described above may not entail the violation of the human dignity of employees and persons employed under any other form of employment legal relationship – therefore the Labour Safety Officer may not abuse his/her surveillance authority, and may not exercise such right in contradiction with its intended purpose, for instance, if such surveillances are conducted several times a day without good reason or in retaliation; it is also unlawful if a person not vested with the appropriate scope of rights would require such testing.

Persons eligible to conduct tests:

- Senior Executive Officer,
- Labour Safety Officer,

- in the case when the Labour Safety Officer is prevented from acting: the Security Guard,
- in the case of tests at the gatekeeper service: the Security Guard.

The Labour Safety Officer may initiate tests with the random sampling method in accordance with his/her authorisation granted in Section 54 (7) b) of Mvt. Tests may be conducted by the Labour Safety Officer him/herself or may be delegated to the Security Guard.

The Security Guard may conduct such tests only in the case of actual suspicion and never with random sampling method.

The exact testing procedure:

- the Labour Safety Officer may at any time request the alcohol testing of any of the employees or other persons employed under any other form of employment legal relationship, even with the random sampling method,
- in the case of suspicion, the Line Manager of the person concerned is obliged to initiate proceedings,
- in response to notice from any of the employees of or persons employed under any other form of employment legal relationship by the Company, the Labour Safety Officer is entitled to request alcohol testing provided that the employees and persons employed under any other form of employment legal relationship could indicate the reason for such testing and the person to be tested, however, the Labour Safety Officer is entitled to refuse such testing if the circumstances giving reason for measures do not suggest unambiguously that such testing would be justified,
- if the labour safety officer is prevented from acting, in response to notice from any of the employees of or persons employed under any other form of employment legal relationship by the Company, a security guard is also entitled to request alcohol testing provided that the employees and persons employed under any other form of employment legal relationship could indicate the reason for such testing and the person to be tested, however, the security guard is entitled to refuse such testing if the circumstances giving reason for measures do not suggest unambiguously that such testing would be justified,
- employees and persons employed under any other form of employment legal relationship should be tested without violating their personal right, in the presence of two witnesses either with alcohol sonde or with breathalyser,
- the person conducting such test should prepare a protocol, the protocol should contain the following: the fact of testing, the circumstance giving reason for testing (general purpose labour safety testing or suspicion of alcohol impairment), the person tested, time of testing, test result, legal declaration of the tested person regarding the result of the testing (accepts or does not accept),
- if an employee or a person employed under any other form of employment legal relationship would not accept the result, he/she may initiate the checking of his/her blood alcohol level by taking blood sample,
- if an employee or a person employed under any other form of employment legal relationship would not cooperate with the Labour Safety Officer and would not wish to undergo testing, the Labour Safety Officer should immediately notify the person who exercises employer's right over such employee,
- refusal of testing automatically qualifies as unfitness for working in accordance with Section 60 (1) of Mvt., because the employee refused his/her statutory cooperation obligation.

If the employee or person employed under any other form of employment legal relationship qualifies unfit for work (positive result or breaching of the cooperation obligation), the person conducting the test is obliged to immediately notify the person vested with employer's right or decision right over the employee or person employed under any other form of employment legal relationship who will then be obliged to

exclude the employee or persons employed under any other form of employment legal relationship from work.

If the test was conducted by the security guard on the basis of suspicion, as soon as the reason that prevented the Labour Safety Officer from acting would cease, the security guard is obliged to immediately notify the Labour Safety Officer on the test performed by him/her and its result.

purpose of data processing: check of fitness for work for labour safety purposes
scope of processed data: result of the test, time, fact of fitness for work, data of the person performing the test, data of the employee or the person employed under any other form of employment legal relationship tested. If the tested person would debate the result, this fact; also, if the test was positive and the employee or persons employed under any other form of employment legal relationship would abandon his/her right for blood test, this fact, too.
legal ground of data processing: Section 60 (1) of Act XCIII of 1993 on Labour Safety and Sections 11 (1) and (2) of Act I of 2012 on Labour Code.
time scope of data storage: the deadline open for enforcing claims grounded by the rights and obligations stemming from testing.
data storage method: in hard copies and electronically.

A detailed information material about the testing procedure has been elaborated for the employees and persons employed under any other form of employment legal relationship which was understood by employees and persons employed under any other form of employment legal relationship. The information material elaborated for employees is attached as Enclosure 5/1 to this Regulation and the information material for persons employed under any other form of employment legal relationship is attached as Enclosure 5/2 to this Regulation.

7.8. Data processing in the course of activities/operation

The Company is the first large civil research institution applying high intensity lasers, which has been established under European cooperation and with the participation of the international scientific community.

In the course of its operation, the Company processes personal data in connection with the following activities:

- operation of visitors' centre
- event organisation
- homepage running
- newsletter distribution
- brand building

Data processing related to the operation of visitors' centre

The research centre may be visited after preliminary notice and registration.

Preliminary application should be submitted 168 hours prior to the visit.

Applications can be submitted through an electronic interface by way of completing data shown in Enclosure 7/3 and furthering the completed document to the following e-mail address: pr@eli-alps.hu.

Preliminary registration is necessary in order to satisfy the obligation to cooperate with authorities.

Keeping contact with the Constitution Protection Office is prescribed in Section 28 (3) of Act CXXV of 1995 on National Security Services (hereinafter: Nbtv.).

In the course of applying for a visit, the following data should be given: name, date of birth and place of birth, mother's name.

The transferred data will be processed by the unit responsible for Security Surveillance.

Personal data captured will be transferred to the Constitution Protection Office which is appropriately authorised by a specific legal rule (Nbtv.) in view of the fact that the research centre qualifies as a facility to be protected for national security reasons according to Government Decree 2009/2015 (XII.29.).

purpose of data processing: enabling visits to the research centre

scope of data processed: name, date of birth and place of birth, mother's name

legal ground of data processing: consent of the data subject given in accordance with Section 5 (1) a) of Act CXII of 2011

time scope of data storage: until the achievement of the intended purpose of data processing but at most one year

data storage method: electronically and in hard copies

A detailed information material describes data processing, its text can be found in Enclosure 7/1 of this Regulation. Data to be submitted in the course of registration should be given in accordance with Enclosure 7/3 of this Regulation.

Data processing in the course of event organisation

The Company organises various events, primarily conferences.

The Company notifies the visitors of such events in advance on the data processing rules relative to them.

purpose of data processing: strengthening the image and the brand of the Company through marketing activities, taking and using video records and photographs on this events in this context.

scope of processed data: voice and image records of data subjects and other data that can be related to the data subjects.

legal ground of data processing: consent given under Section 5 (1) a) of Infotv., and Section 2:48 (1) of Act V of 2013 on the Civil Code

time scope of data storage: until the achievement of the intended purpose of the marketing activity, but at most one year

data storage method: electronically and in hard copies

The utilisation of video records and photographs taken in the course of events are described in a data controlling information leaflet, which is attached as Enclosure 8 to this Regulation.

Participation in certain events is conditional upon preliminary registration.

In the course of registration the following data are requested from applicants:

name, place of birth, date of birth, mother's name, name of the institution represented by the applicant, position of the applicant, e-mail address, if the applicant arrives by vehicle and requests parking lot: the

registration number of the vehicle, furthermore a declaration from the applicant that he/she wishes to visit the visitors' centre.

purpose of data processing: identification of the participant of the event

scope of processed data: name, place and date of birth, mother's name of the applicant, name of the institution represented by the applicant, position of the applicant, e-mail address, registration plate of the vehicle (if the applicant arrives by vehicle and requests parking lot), declaration from the applicant that he/she wishes to visit the visitors' centre.

legal ground of data processing: consent of the data subject in accordance with Section 5 (1) a) of Infotv.

time scope of data storage: until the finalisation of the event

data storage method: electronically

The declaration of consent related to the processing of data captured in the course of events conditional upon registration is attached as Enclosure 9 to this Regulation.

Data processing related to the running a homepage

The Company has its own homepage, its address is:

http://www.eli-hu.hu/

The homepage operated by the Company can be accessed by anyone without revealing his/her identity and giving his/her personal data, also, information can be retrieved from the homepage and the linked sites freely and without restrictions. Meanwhile the homepage gathers non-personal information about its visitors without any restriction. From these pieces of information personal data cannot be retrieved, therefore this is not constituted as data controlling coming under the scope of Infotv.

On its homepage the Company utilises a web analytics service named Google Analytics. Google Analytics applies cookies and text files downloaded on the computer of the visitor of the website, the aim of which is the facilitation of the analysis of the use of the website. Pieces of information generated by the cookies and related to the use of the website (IP-address of the visitor of the website) are transferred to the server of Google located in the United States of America and are stored there. Google does not interconnect information generated by the cookies with other data, therefore, according to the data protection regulation in force it cannot be deemed to be data processing. By way of appropriately setting his/her browser, the visitor of the website can refuse the application of cookies. By virtue of using the website, the visitor of the homepage consents the processing of his/her data in the manner and/or the purpose as discussed above.

Pieces of information so acquired are used by Google for the evaluation of the use of the homepage by data subjects, for analyses, compilation of reports on operations performed on the website, and for delivering other services related to operations performed on the homepage and to internet usage.

If any operation on the homepage requires logging in, the Company handles personal data of the visitors in the following manner:

purpose of data processing: identification of the visitors of the homepage; making electronic services available for them

scope of processed data: starting and finishing time of the visit of the user, and/or in certain cases – dependently upon the settings of the user's computer – the type of the browser and the operating system,

IP address, other captured data (cookies) in the case of operation requiring logging in: name, e-mail address,

legal ground of data processing: consent of the data subject in accordance with Section 5 (1) a) of Infotv.

time scope of data storage: until the achievement of the purpose of data processing, for maximum 2 years

data storage method: electronically

A data protection information material has been elaborated on data processing in connection with the homepage, which is attached as Enclosure 10 to this Regulation.

Data processing in connection with newsletter distribution

The Company ensures possibility for interested parties to subscribe for newsletters if they so demand, and therefore they can be provided with information concerning the operation and activities of the Company and other interesting news. The data subjects may unsubscribe from the newsletter at the following e-mail address: .....

purpose of data processing: newsletter distribution for subscribers

scope of processed data: user name, e-mail address

legal ground of data processing: consent of the data subject in accordance with Section 5 (1) a) of Infotv.

time scope of data storage: until the data subject would unsubscribe.

data storage method: electronically

Data protection information material has been elaborated in respect of data processing in connection with newsletter distribution, which is attached as Enclosure 11 to this Regulation.

Data processing related to brand building

From time to time the Company send its representatives to certain events: job exchange, industry days, festivals. In such events the Company ensures possibilities for the visitors of its stand to participate in games organised by the Company, such as the completion of a quiz related to the Company's activities. Name and contact data of persons completing the quiz in the game organised during the event are captured and are used for notifying winners of the sweepstakes.

purpose of data processing: organisation and arrangement of sweepstakes

legal ground of data processing: consent of the data subject in accordance with Section 5 (1) a) of Act CXII of 2011

scope of processed data: name, telephone number and e-mail address

time scope of data controlling: until the notification of the winner

data storage method: in hard copies and electronically

Data protection information material has been elaborated regarding the processing of data captured in the course of sweepstakes, which is attached as Enclosure 12 to this Regulation.

7.9. Application of electronic surveillance system

The Company applies closed circuit camera surveillance system in its site under 5 Budapesti Street, Szeged.

The cameras form the Company's own property and are operated by the Company.

The camera records are stored on the local servers.

In the case of terror hazard the Constitution Protection Office may have access to the records in view of the fact that the site is a distinguished national security facility.

Sectors of the electronic surveillance system

The Company distinguishes the areas watched by the electronic surveillance system into two separate categories according to the aim of surveillance.
The first category is the so-called sector I where the legal rule that governs the applied electronic surveillance system is Section 31 (3) c) of Szvtv., because the aim of surveillance is the safe storage, handling and transportation of properties and equipments, money, securities, noble metal, precious stones that are of at least significant value as described in the Act on the Criminal Code.

The second category is the so-called sector II where the legal rules that governs the applied electronic surveillance system is Section 31 (3) d) of Szvtv., because the aim of the surveillance is the safeguarding of hazardous materials.

Method of and deadline set for erasure of records generated by the electronic surveillance system

Sector I
As per Section 31 (3) c) of Szvtv. at the units specified by the Company, because the aim of surveillance is the safe storage, handling and transportation of properties and equipments, money, securities, noble metal, precious stones that are of at least significant value as described in the Act on the Criminal Code.

Sector II
As per Section 31 (3) d) of Szvtv., records taken in the interest of safeguarding hazardous materials are kept by the Company for 30 days.

In both cases the Company from among the rights that the data subjects are vested with guarantees those specified in Szvtv., i.e. if a record interferes with a person's rights or lawful interests, such person may within the deadline set for erasure as specified above (thirty days) request the data controller not to destroy and/or not to erase such record provided that he/she can certify his/her right or legal interest. The decision about such request will be passed by the internal Data Protection Officer of the Company within the shortest possible deadline. The record so distinguished should be saved and handed over to the internal Data Protection Officer who will arrange for its safeguarding in accordance with the data protection rules corresponding with this present Regulation. In response to any request from a court or other authority, the record should be sent to the court or authority without delay. If such request would not be received within thirty days from the day when the request for disregarding destruction was received, such record will be erased.

Warranty rules related to electronic surveillance

Through the electronic surveillance system, the Company interferes with the privacy of the data subject only to the necessary extent.

The Company does not apply electronic surveillance for whatever reason and in whatever manner in the following cases:

- surveillance of the work intensity of the employee,
- influencing the behaviour conducted by employees at the work premises,
- in sensitive areas, specifically changing room, shower, toilette,
- in areas where employees spend their relax time or breaks, specifically relaxation rooms, smoking areas,
- public areas.

However, the Company may apply electronic surveillance in order to gain confidence that the employees observe the regulations related to them in the interest of health safe and secure work practices.

Information given to the data subjects

An information material has been elaborated regarding the data processing with the aim of giving preliminary information to the data subjects on data processing. This information material is attached as Enclosures 13/1 and 13/2 of the Regulation. The information materials are posted at the points of entry of all watched areas and at the points of crossing between categories I and II.

Information for the employees of and persons employed under other form of employment legal relationship by the Company

An information material is addressed to the employees regarding data processing with the aim of providing employees and persons employed under any other form of employment legal relationship with preliminary information about data processing. The text of the information material is included in Enclosures 5/1 and 5/2 of this Regulation.

Viewing images recorded by the cameras

In order that the Company would interfere with the privacy of the data subjects to the least extent, the images recorded by the electronic surveillance system may be accessed by designated persons only.

Within the organisational system of the Company, only the person designated in this present Regulation may view recorded images.

In the course of electronic surveillance applied by the Company, only persons listed in Enclosure 14/1 of this Regulation are vested with right to view.
A protocol should be taken on viewing images recorded by the cameras, which is attached as Enclosure 14/2 to this Regulation.

Blocking of camera images

Blocking of images taken by the cameras may be required only by a person designated to supervise data processing through the Company's camera system.

Blocking of camera images may be initiated by:

- a person vested by the Company with right to view if in the course of viewing such images he/she would perceive any circumstance that would endanger the aim to be achieved by the electronic surveillance system,
- anybody, whose rights or lawful interests are interfered by the records.

Blocking of the camera records can be requested with an application addressed to the person designated to supervise data processing through the camera system and concurrently to the internal data protection officer if such person has been designated.

The decision about blocking will be passed by the person designated by the company for supervising data processing through the camera system within the shortest possible time (in agreement with the internal Data Protection Officer if such person has been designated).

The Company takes a protocol on blocking images recorded by the cameras, in which the time of viewing and blocking, its purpose furthermore the event giving reason for blocking and the indication of further use should be stated.
The relevant protocol is attached as Enclosure 15/1 of this Regulation.

Persons vested with blocking eligibility

The Company keeps a registry on the scope of persons entitled to block images. Such registry contains the name and position of the person vested with blocking rights, date of issuing such blocking right, date of withdrawal of blocking right. The Company keeps such data for 5 years counted from withdrawal. The record of persons vested with blocking eligibility is attached as Enclosure 15/2.

Sector I
purpose of data processing: storage, handling and transportation of properties and equipments, money, security, noble metal, precious stone qualifying as at least of significant value according to the Act on the Criminal Code.
scope of processed data: portrait of the data subject, data that can be acquired with the camera image (place of stay, duration of stay),
legal ground of data processing: implied consent of the data subject [Section 30 (2) of Szvtv.]
time scope of data storage:

- if the record is not utilised, it will be erased within 30, say thirty days passing from recording [Section 31 (3) c) of Szvtv.]
- if following the certification of rights of lawful interests, the Company was requested not to destroy the record, meanwhile, request was not submitted, then the record will be erased within 30, say thirty days from such request [Section 31 (6) of Szvtv.]

method of data processing: electronically

Sector II
purpose of data processing: safeguarding hazardous materials
scope of processed data: portrait of the data subject, data that can be acquired with the camera image (place of stay, duration of stay),
legal ground of data processing: implied consent of the data subject [Section 30 (2) of Szvtv.]

- if the record is not utilised, it will be erased within 30, say thirty days from recording *[Section 31 (3) d) of Szvtv.]*
- if following the certification of rights of lawful interests, the Company was requested not to destroy the record, meanwhile, request was not submitted, then the record will be erased within 30, say thirty days passing from such request [Section 31 (6) of Szvtv.]

method of data processing: electronically

7.10. Management of extraordinary security events

Extraordinary event shall mean an event or circumstance that deviates from the average, which therefore may lead to severe consequences regarding life, corporeal integrity of persons staying in the facility or regarding properties to be found there, or there are realistic chances for leading to such consequences and therefore severe disturbance in the operation of the facility could be caused.

The Security Guards employed by the contracted service provider will take protocol on any event within the premises that is of relevance from the security aspect. Such protocol should contain the following data: date of taking protocol, name of the member of the staff of the security service, his/her signature, name of the person investigated, his/her signature, name at birth, place, date of birth, mother's name, residential address, place of stay of the person investigated and the description of the event. These data are relative personal data, therefore – under Infotv. – they might become personal data.

purpose of data processing: investigation of extraordinary security event
scope of processed data: date of capturing the protocol, name of the member of the staff of the security service, his/her signature, name of the person investigated, his/her signature, name at birth, place and time of birth, mother's name, residential address, place of stay of the person investigated and the description of the event
legal ground of data processing: consent of the data subject in accordance with Section 5 (1) a) of Infotv.
time scope of data storage: investigation of the event, the deadline available for enforcing claims regarding rights and obligations stemming therefrom.
data storage method: in hard copy

7.11. Security surveillances

In the interest of protecting properties, on the basis of the authorisation ensured by Section 26 of Szvtv., the Company conducts package, cabinet/locker, vehicle and cargo surveillance.

Such surveillance may be conducted by the Security Guard for the purpose of enforcing his/her obligations stemming from the contract, following notification as regards the reason and the aim of the measure, in those cases when

- it can be suspected with good ground that the person concerned keeps a thing acquired by criminal action or misdemeanour, and the safeguarding of such property is the contractual obligation of the Security Guard,
- such thing is not handed over despite the relevant request, and
- such measure is necessary for preventing or halting a law violating act.

If the surveillance is closed with tangible result, the Security Guard takes a protocol on the surveillance of the extraordinary event, and such protocol will be subjected to the relevant rules of data processing (point 7.10. of the Regulation).

7.12. Access control

The facility in Szeged (6728 Szeged, 5 Budapesti Street) is separated to several zones from the security and access eligibility aspects.

The green zone is the area that is open for clients; this area may be accessed by anyone without authentication of identity or any check.

The yellow zone is the area of the visitors' centre where visitors may enter following preliminary registration. After the authentication of the identity, the visitor will be provided with a badge. Registration will be executed in accordance with the provisions stipulated in the chapter about the visitors' centre.

Into the area of the orange zone exclusively employees and persons employed under other form of employment relationship and their visitors may enter.

The red zone is intensely protected, it may be accessed by a narrow scope of employees (e.g. server room, security surveillance, etc.).

The black zone is the so-called laser space. This area may be accessed only by persons vested with distinguished access rights.

The white zone is a separated area where the kitchen can be found which is operated by an external firm.

An information material has been elaborated about the access control process which is attached as Enclosure 16 to this Regulation.

Control of access by employees and persons employed under any other form of employment legal relationship

The rights to access premises of the Company vary with the individual jobs/positions.

Employees and persons employed under other form of employment relationship may move amongst the zones in correspondence with the eligibility levels shown on their entry card.

The card shows the name, card number and a photograph.

The access control system – and therefore the access control database – is operated by the Company. The entry data are stored on the Company's server.

purpose of data processing: security surveillance conducted in the course of controlling entrances and departures

scope of processed data: name, time of entrance/departure, identification number of the entering person

legal ground of data processing: consent of the data subject in accordance with Section 5 (1) a) of Infotv. and Section 32 of Act CXXXIII of 2005.

time scope of data storage:

- in the case of eligibility for regular entrances, the authentication data (name and identification number) necessary for the operation of the system will be deleted by the Company immediately after the termination of such eligibility,
- in the case of eligibility for regular entrances, those data that were generated in the course of the operation of the system will be deleted concurrently with the termination of such eligibility but latest after 6 months from the generation of such data.

data storage method: electronically

A detailed information material has been elaborated for employees and persons employed under other form of employment relationship about the access control process and the data subjects have familiarised themselves with that. This information material is attached as Enclosures 5/1 and 5/2.

Access control for suppliers

In the case of suppliers, in accordance with the AEO (Authorised Economic Operator) standard, the data of the entering persons should preliminarily be submitted to the gatekeepers: name of the driver, mother's name (in certain cases father's name), date of birth, place of birth, vehicle registration number and the data of the cargo.

Data in such cases are captured in hard copy by the gatekeeper service.

purpose of data processing: security surveillance in the course when suppliers access the premises

scope of processed data: name of the driver, mother's name (in certain cases father's name), date of birth, place of birth, vehicle registration number and the data of the cargo.

legal ground of data processing: the consent of the data subject in accordance with Section 5 (1) a) of Infotv. and Section 32 of Act CXXXIII of 2005.

time scope of data storage:

identification data handled for access controlling purposes should be destroyed

- in the case of eligibility for regular entrances immediately after the termination of such eligibility,
- in the case of occasional entries after 24 hours passing from departure

data storage method: in hard copy

ENCLOSURES

Enclosure No. 1

DYNAMICALLY CHANGING ELEMENTS OF THE REGULATION

Processing of data of persons aspiring for work
Data processor and data transfer is not involved in this data controlling

Data processing related to employment relationship

Data transfer for health funds:

- **Allianz Hungária Health and Mutual Fund** (.....)
  activities involving data processing: provision of cafeteria services
  legal ground of data transfer: consent granted by the data subject on the basis of Section 12 of Act XCVI of 1993 on voluntary mutual funds
  scope of transferred data: name, address, tax number, bank account number of the employee, name and tax number of the beneficiary

- **Dimenzió Voluntary Mutual Health Fund** (.....)
  activities involving data processing: provision of cafeteria services
  legal ground of data transfer: consent granted by the data subject on the basis of Section 12 of Act XCVI of 1993 on voluntary mutual funds
  scope of transferred data: name, address, tax number, bank account number of the employee, name and tax number of the beneficiary

- **Generali Health and Mutual Fund** (.....)
  activities involving data processing: provision of cafeteria services
  legal ground of data transfer: consent granted by the data subject on the basis of Section 12 of Act XCVI of 1993 on voluntary mutual funds
  scope of transferred data: name, address, tax number, bank account number of the employee, name and tax number of the beneficiary

- **Medicina Health Fund** (.....)
  activities involving data processing: provision of cafeteria services
  legal ground of data transfer: consent granted by the data subject on the basis of Section 12 of Act XCVI of 1993 on voluntary mutual funds
  scope of transferred data: name, address, tax number, bank account number of the employee, name and tax number of the beneficiary

- **MKB Health Fund** (.....)
  activities involving data processing: provision of cafeteria services
  legal ground of data transfer: consent granted by the data subject on the basis of Section 12 of Act XCVI of 1993 on voluntary mutual funds
  scope of transferred data: name, address, tax number, bank account number of the employee, name and tax number of the beneficiary

- **OTP National Health Fund** (.....)
  activities involving data processing: provision of cafeteria services
  legal ground of data transfer: consent granted by the data subject on the basis of Section 12 of Act XCVI of 1993 on voluntary mutual funds
  scope of transferred data: name, address, tax number, bank account number of the employee, name and tax number of the beneficiary

- **Patika Health Fund (.....)**
  activities involving data processing: provision of cafeteria services
  legal ground of data transfer: consent granted by the data subject on the basis of Section 12 of Act XCVI of 1993 on voluntary mutual funds

scope of transferred data: name, address, tax number, bank account number of the employee, name and tax number of the beneficiary

- **Prémium Health Fund (.....)**
  activities involving data processing: provision of cafeteria services
  legal ground of data transfer: consent granted by the data subject on the basis of Section 12 of Act XCVI of 1993 on voluntary mutual funds
  scope of transferred data: name, address, tax number, bank account number of the employee, name and tax number of the beneficiary

- **Tempo Voluntary Supplementary Health Fund (.....)**
  activities involving data processing: provision of cafeteria services
  legal ground of data transfer: consent granted by the data subject on the basis of Section 12 of Act XCVI of 1993 on voluntary mutual funds
  scope of transferred data: name, address, tax number, bank account number of the employee, name and tax number of the beneficiary

- **Vitamin Health Fund (.....)**
  activities involving data processing: provision of cafeteria services
  legal ground of data transfer: consent granted by the data subject on the basis of Section 12 of Act XCVI of 1993 on voluntary mutual funds
  scope of transferred data: name, address, tax number, bank account number of the employee, name and tax number of the beneficiary

- **Pannónia Health and Mutual Fund (.....)**
  activities involving data processing: provision of cafeteria services
  legal ground of data transfer: consent granted by the data subject on the basis of Section 12 of Act XCVI of 1993 on voluntary mutual funds
  scope of transferred data: name, address, tax number, bank account number of the employee, name and tax number of the beneficiary

Data transfer for pension funds:

- **Aegon Voluntary Pension Fund**
  activities involving data processing: provision of cafeteria services
  legal ground of data transfer: consent of the data subject
  scope of transferred data: name, address, tax number, bank account number of the employee, name and tax number of the beneficiary

- **Allianz Hungária Voluntary Pension Fund**
  activities involving data processing: provision of cafeteria services
  legal ground of data transfer: consent of the data subject
  scope of transferred data: name, address, tax number, bank account number of the employee, name and tax number of the beneficiary

- **Aranykor Voluntary Pension Fund**
  activities involving data processing: provision of cafeteria services
  legal ground of data transfer: consent of the data subject
  scope of transferred data: name, address, tax number, bank account number of the employee, name and tax number of the beneficiary

- **CIB Voluntary Mutual Pension Fund**
  activities involving data processing: provision of cafeteria services
  legal ground of data transfer: consent of the data subject
  scope of transferred data: name, address, tax number, bank account number of the employee, name and tax number of the beneficiary

- **Dimenzió Insurance Mutual**
  activities involving data processing: provision of cafeteria services
  legal ground of data transfer: consent of the data subject
  scope of transferred data: name, address, tax number, bank account number of the employee, name and tax number of the beneficiary

- **Budapest Voluntary Pension Fund**
  activities involving data processing: provision of cafeteria services
  legal ground of data transfer: consent of the data subject
  scope of transferred data: name, address, tax number, bank account number of the employee, name and tax number of the beneficiary

- **MKB Pension Fund**
  activities involving data processing: provision of cafeteria services
  legal ground of data transfer: consent of the data subject
  scope of transferred data: name, address, tax number, bank account number of the employee, name and tax number of the beneficiary

- **OTP Voluntary Pension Fund**
  activities involving data processing: provision of cafeteria services
  legal ground of data transfer: consent of the data subject
  scope of transferred data: name, address, tax number, bank account number of the employee, name and tax number of the beneficiary

- **Pannónia Pension Fund**
  activities involving data processing: provision of cafeteria services
  legal ground of data transfer: consent of the data subject
  scope of transferred data: name, address, tax number, bank account number of the employee, name and tax number of the beneficiary

- **Prémium Voluntary Pension Fund**
  activities involving data processing: provision of cafeteria services
  legal ground of data transfer: consent of the data subject
  scope of transferred data: name, address, tax number, bank account number of the employee, name and tax number of the beneficiary

Data Transfer for issuers of SZÉP card:

- **K&H SZÉP card**
  activities involving data processing: SZÉP card issue
  legal ground of data transfer: consent of the data subject
  scope of transferred data: name, tax identifier, personal ID number, mother's name, place and date of birth, residential address; in the case of applying for partner-card: name of the owner of the partner-card, degree of relationship with the employee

- **OTP SZÉP card**
  activities involving data processing: SZÉP card issue
  legal ground of data transfer: consent of the data subject
  scope of transferred data: name, tax identifier, personal ID number, mother's name, place and date of birth, residential address; in the case of applying for partner-card: name of the owner of the partner-card, degree of relationship with the employee

- **MKB SZÉP card**
  activities involving data processing: SZÉP card issue
  legal ground of data transfer: consent of the data subject
  scope of transferred data: name, tax identifier, personal ID number, mother's name, place and date of birth, residential address; in the case of applying for partner-card: name of the owner of the partner-card, degree of relationship with the employee

Data transfer for travel offices:

OTP Travel Kft. (1051 Budapest, Nádor u. 21.)
WECO Travel Kft. (1053 Budapest, Szép u. 2.)
IBUSZ Utazási Irodák Kft. (Budapest, Dayka G. u. 3.)

legal ground of data transfer: statutory authorisation [Sections 31 and 32 of Kbt. and Section 10 (1) and (2) of Mt], and the consent of the data subject [Sections 5 (1) a) and 6 (6) of Infotv.].
scope of transferred data:
name of traveller, date of birth, place of birth, mother's name, permanent place of residence, tax identification mark, citizenship, passport number, number and validity of passport, issuing authority

Processing of data of relatives in connection with employment relationship
Data processor and data transfer is not involved in this data controlling

Processing of data related to employment under other employment relationship
Data processor and data transfer is not involved in this data controlling

Data processing in connection with the surveillance of the technical devices of employees
Data processor and data transfer is not involved in this data controlling

Data processing in connection with the surveillance of the technical devices of persons employed under other form of employment legal relationship
Data processor and data transfer is not involved in this data controlling

Surveillance of conditions fit for work from the labour safety aspect
Data processor and data transfer is not involved in this data controlling

Data processing procedures in the course of activities/operation
Data processing related to the operation of the visitors' centre
Data processing in the course of event organisation
Data processing in connection with the running a homepage
Data processing related to newsletter distribution
Data processing in connection with brand-building

Data processing and data transfer are not involved in these data controlling processes

Application of electronic surveillance system
Sector I
Sector II

Data transfer:
Constitution Protection Office
activity related to data control: viewing recorded images in the case of terror threat
legal ground of data transfer: Section 28 (3) of Act CXXV of 1995, Government Decree 009/2015 (XII.29.)
scope of transferred data: portrait, place of stay
Handling extraordinary security events
Currently data processor and data transfer is not involved in this data control
Access control
Entrance of employees
Currently data processor and data transfer is not involved in this data control
Person responsible for internal protection of data: with effect of the day when this regulation enters into force: dr. Viktória Papp,
e-mail address: adat@eli-alps.hu

Enclosure No. 2

DATA PROTECTION REGISTRATION NUMBERS

a) Data processing in connection with the data of persons applying for job

registration number of the data processing: NAIH-114177/2017.

b) Data processing in connection with employment relationship

registration number of the data processing: under Section 65 (3) a) of the Info Act, the National Authority for Data Protection and Freedom of Information does not include this data processing in its registry because that is related to data of persons in employment relationship with the data controller

c) Processing of data of relatives in connection with employment relationship

registration number of the data processing: under Section 65 (3) a) of the Info Act, the National Authority for Data Protection and Freedom of Information does not include this data processing in its registry because that is related to data of persons in employment relationship with the data controller

d) Data processing in connection with employment under other employment relationship

registration number of the data processing: under Section 65 (3) a) of the Info Act, the National Authority for Data Protection and Freedom of Information does not include this data processing in its registry because that is related to data of persons in employment relationship with the data controller

e) Data processing in connection with the surveillance of the technical devices of employees

registration number of the data processing: under Section 65 (3) a) of the Info Act, the National Authority for Data Protection and Freedom of Information does not include this data processing in its registry because that is related to data of persons in employment relationship with the data controller

f) Data processing in connection with the surveillance of the technical devices of persons employed under other form of employment legal relationship

registration number of the data processing: under Section 65 (3) a) of the Info Act, the National Authority for Data Protection and Freedom of Information does not include this data processing in its registry because that is related to data of persons in employment relationship with the data controller

g) Surveillance of fitness for work from the labour safety aspect

registration number of the data processing: under Section 65 (3) a) of the Info Act, the National Authority for Data Protection and Freedom of Information does not include this data processing in its registry because that is related to data of persons in employment relationship with the data controller

h) Data processing in the course of activities/operation

- **Data processing in the course of the operation of visitor's centre**
  registration number of the data processing: under Section 65 (3) a) of the Info Act, the National Authority for Data Protection and Freedom of Information does not include this data processing in its registry because that is related to data of persons in client relationship with the data controller

- **Data processing in the course of event organisation**

registration number of the data processing: NAIH-114080/2017.

- **Events with registration obligation**
  registration number of the data processing: under Section 65 (3) a) of the Info Act, the National Authority for Data Protection and Freedom of Information does not include this data processing in its registry because that is related to data of persons in client relationship with the data controller

- **Data processing in connection with homepage running**
  registration number of the data processing: under Section 65 (3) a) of the Info Act, the National Authority for Data Protection and Freedom of Information does not include this data processing in its registry because that is related to data of persons in client relationship with the data controller

- **Data processing related to newsletter distribution**
  registration number of the data processing: NAIH-114082/2017.

- **Data processing related to brand-building**
  registration number of the data processing: NAIH-114083/2017.

i) Application of electronic surveillance system

Sector I: **registration number of the data processing: NAIH-114084/2017.**

Sector II: **registration number of the data processing: NAIH-114085/2017.**

j) Management of extraordinary security events

registration number of the data processing: NAIH-114086/2017.

k) Access control

- **Employees' access to the premises**:
  registration number of the data processing: NAIH-114087/2017.

- **Suppliers' access to the premises: registration number of the data processing: NAIH-114176/2017.**

Enclosure No. 3

DECLARATION OF CONFIDENTIALITY

By virtue of this declaration hereby we confirm our agreement and understanding, namely that certain information that has already been or will in the future be discovered by **ELI-HU Research and Development Non-profit Llc.** to ..... (name) (..... – mother's name, place and date of birth) specifically business plans, trade secrets, clients' data and other proprietary information, personal data coming under the scope of Act CXII of 2011 on Right of Informational Self-Determination and Freedom of Information (hereinafter together: information) are of confidential nature.

By virtue of signing this declaration ..... undertakes not to publish, not to make available or not to reveal in any other manner any part or fragment of such information for any third party without the preliminary written consent given in this respect by the Senior Executive Officer of **ELI-HU Research and Development Non-profit Llc.**, except if such information can be published as a document of probative force. Such pieces of information may not be deemed as publishable solely for that reason that further general information can be obtained from them or because they can be collected from one or more other sources, or if they have become public domain because this declaration or a similar declaration made for a third party or for a legal person has been breached.

The person making this declaration agrees that he/she will do everything and take all reasonable precautionary measures in order to ensure appropriate protection for all such information revealed either verbally, or in hard copy or on electronic data media or in any other manner, in order to prevent unauthorised revealing for third parties, specifically he/she will observe the provisions of governing force stipulated in the Data Protection Regulation of **ELI-HU Research and Development Non-profit Llc.** Also he/she agrees that he/she will not make copy of any documents, and will return any copies in response to the relevant request.

Furthermore, the person making this declaration acknowledges that all such information is the property of **ELI-HU Research and Development Non-profit Llc.**, and in the interest of the continuous business conduct of the **Llc.** all pieces of information are confidential, valuable and indispensable. He/she agrees that he/she will not utilise or exploit such information and/or place them on business grounds for his/her own benefit or for the benefit of any other third party.

By virtue of signing this declaration, the person named above is not vested with any eligibility or right.

This present declaration of confidentiality will enter into force on ..... (date or a specific event, such as e.g. "simultaneously with the signature of the employment contract").

Any personal data coming under the scope of Act CXII of 2011 given in this present declaration of confidentiality will be processed by **ELI-HU Research and Development Non-profit Llc.** in accordance with the Data Protection Regulation.

Szeged, ... 20.....

_____	_____
Declarer	representing ELI-HU Research and Development Non-profit Llc.

Enclosure 4/1

RESPONSE LETTER TO RESUMES INCLUDED IN THE DATABASE

Dear .....,

Thank you for sending your resume to **ELI-HU Research and Development Non-profit Llc.** Please be informed that currently we do not have any vacant position[1] that would match your capabilities/you are not among the candidates selected for filling the advertised position[2].

However, as regards the future, we hope that we could offer you a position that matches your capabilities and experiences. In view of this, on the basis of point 7.1 of the Data Protection Regulation of the Company, your resume will be filed and categorised in the interest of occasional future utilisation, in order that should we seek a prospective employee for a job that is appropriate for you, you also could be included among the prospective candidates.

Accordingly, your resume and all personal data included therein will be captured on the legal ground specified in Section 6 (6) of Act CXII of 2011 on Right of Informational Self-Determination and Freedom of Information, in order to facilitate the selection of appropriate employees, and will be kept in our records in accordance with the rules related to personal data of candidates aspiring for jobs stipulated in the Data Protection Regulation of the Company.

You, of course, may request the erasure of your personal data any time, please address your application to the Company's employee responsible for data protection or to the HR Expert.
The Company's Data Protection Officer is Dr Viktória Papp, e-mail address: adat@eli-alps.hu
The company's HR Expert is Diána Tóth, e-mail address: diana.toth@eli-alps.hu

May we trust that we could greet you among our employees sometimes in the future. Also, we hope that further on you are going to monitor job possibilities advertised by us.

On behalf of **ELI-HU Research and Development Non-profit Llc.** we would like to thank you for your confidence and interest in our Company, and wish you many successes in the achievement of your goals.

....., ... 20.....

Yours sincerely,

[1] in the case of unsolicited resume
[2] in the case of aspiration for specific position

Enclosure No. 4/2

RESPONSE LETTER TO RESUMES RECEIVED NOT FROM THE PERSON CONCERNED

Dear .....,

Please be informed that your resume was received through xXx. In accordance with our Data Protection Regulation, xXx made a declaration concerning the authorisation you have given to him/her to submit your data to us.

However, in order that the Company would not commit law violation, you are kindly requested that should you not have given authorisation to xXx for revealing your data for us, please notify us and we will take measures regarding the erasure of your data.
Should you request the erasure of your personal data, please address your application to the Company's employee responsible for data protection or to the HR Expert.

The Company's Data Protection Officer: Dr Viktória Papp, e-mail address: adat@eli-alps.hu
The company's HR Partner: Diána Tóth, e-mail address: diana.toth@eli-alps.hu

If you have given your consent to the processing of your data, we would like to inform you as follows: we hope that we could be able to offer you a position that is in correspondence with your capabilities and experiences. In view of that, on the basis of point 7.1 of the Data Protection Regulation of the Company, your resume will be filed and categorised for the purpose of eventual future utilisation and in case we would search for a prospective employee for a job that is satisfactory for you, you could be included among the possible candidates.

Accordingly, your resume and all personal data included therein, on the ground specified in Section 6 (6) of Act CXII of 2011 on Right of Informational Self-Determination and Freedom of Information will be captured in order to facilitate the selection of appropriate employees, and afterwards, in accordance with the Data Protection Regulation of the Company will be kept in our records on the basis of rules related to the personal data of candidates for job.

We trust that we can greet you among our employees in the future. We hope that further on you will monitor job possibilities advertised by us.

On behalf of **ELI-HU Research and Development Non-profit Llc.** we thank you for your confidence and interest and wish you success in the achievement of your goals in the future.

....., ... 20.....

Yours sincerely,

Enclosure No. 4/3

DECLARATION OF THE EMPLOYEE AT MAKING RECOMMENDATION (CV)

Name of employee:	
Individual identifier of the employee:	
Name of the recommended person:	
Place and date of birth of the recommended person:	
Date of recommendation:	

By virtue of my signature, under civil and criminal liability of perjury, hereby I declare that I am authorised by the person recommended by me that I could reveal his/her personal data for **ELI-HU Research and Development Non-profit Llc.** and submit his/her resume to the Company.

....., ... 20.....

signature

Enclosure No. 5/1

DATA PROTECTION INFORMATION MATERIAL FOR EMPLOYEES

This present information material qualifies as preliminary information in accordance with Act I of 2012 on the Labour Code **(hereinafter Mt.), Section 9 (2)** *[„The personal right of workers may be restricted if deemed strictly necessary for reasons directly related to the intended purpose of the employment relationship and if proportionate for achieving its objective. The means and conditions for any restriction of personal rights, and the expected duration shall be communicated to the workers affected in advance."],* **Section 11 (2) of Mt.** *[„Employers shall inform their workers in advance concerning the technical means used for the surveillance of workers."]* and **Section 10 (2) of Mt.** *[„Employers shall inform their workers concerning the processing of their personal data"].*

DATA PROCESSING RELATED TO EMPLOYMENT RELATIONSHIP

The aim of the data processing related to employment relationship is the establishment, maintenance and termination of employment relationship.

Handling judicial records

In order to comply with the provisions stipulated in the legal rules and to meet commitments under other legal relationships, the Company reserves the right to hire employees who comply with its moral expectations, therefore the Company may make the employment conditional upon clean judicial records.

Clean judicial record will be checked by the HR partner who will verify the:

- validity (in a manner available for anyone), and
- content of the judicial record.

The Company may handle personal data processed in criminal matters only with the written consent of the data subject. The Company preliminarily notifies the data subject about the reason for handling personal data processed in criminal matters, which is making a decision about data subject's worthiness for the given position; therefore such data will be handled until this purpose would be achieved, until the passing of the decision.

The Company requests clean criminal record as a condition for filling a given specific job. In cases deserving special consideration, the Company's Senior Executive Officer, in the course of individual evaluation may make positive decision concerning worthiness for a given job if according to the judicial record:

- the nature and severity of the act committed is not irreconcilable with the expectations related to the job to be filled,
- court exoneration is in progress,
- statutory exoneration is opportune,
- there are other reasons deserving special consideration which guarantee that the Company's mission and principles would be not endangered.

In the course of aspiring for a job, data are transferred to the person vested with decision right on the ground discussed hereunder. The evaluation of the aptitude for the job is the responsibility of the back office whilst in the case of Engineers the responsibility is burdened on the Professional Managers and the HR expert. Data given in the course of application for a job could therefore be known not only by the Professional Managers and the HR Expert, but – in the special case described above – by the Senior Executive Officer of the Company, too.

The data may not be known by others than those indicated above, therefore other employees of the Company or any other person having legal relationship with the Company may not have access to such data in any manner or form.

In the course of the establishment of an employment relationship in respect of a given job, the data subject submits his/her valid judicial record. In view of the fact that the worthiness for the job is decided by the Professional Managers and the HR Expert, all of the data must be transferred to them. However, the Company in all cases seeks the best method for not restricting the privacy of the data subject and in consideration of the fact that a valid judicial record may within 90 days from its issue be used for purposes other than applying for a job with the Company, the Company physically does not file the judicial record of the data subject.

In order to achieve that data shown on the judicial record could be accessed only by the competent person, the Company obligatorily requests that in the course of the recruitment procedure the judicial record could be revealed by the applicant only for the Professional Managers and the HR Expert and – in the special case described in this present point – for the Company's Senior Executive Officer.

In the cases deserving special consideration, if in the course of the procedure aimed at the establishment of employment relationship, the data subject cannot present his/her judicial record, such judicial record may be mailed to the company in order to make documentation complete. In such case within a deadline of 30 days

- the Professional Manager makes decision on the employment relationship,
- the document will after the closure of the decision process be successively sent back to the data subject in a traceable manner.

In order that the Company could prove

- that in the course of the recruitment process, it has inspected the validity of the judicial record,
- what sort of available data were used for the evaluation of the prospective employee in the course of the recruitment process,
  together with the data necessary for the maintenance of the employment relationship, the following data will also be captured in the same manner and with the same storage deadline:
  - date of issue of the judicial record
  - deed number of the judicial record
  - identifier of the application for judicial record.

However, according to the legal rules these data do not qualify as special/sensitive personal data because they are not personal data processed in criminal matters. On the basis of the data mentioned above, the genuineness and the content of judicial records issued after 1 January 2013 can be successively verified in the system of KEKKH.

Therefore the Company does not store any judicial record either in the course of the recruitment procedure or during the employment relationship and does not make copy of the judicial record.

In the event when a given person aspiring for a job would not be selected, his/her data i.e. data related to his/her judicial records will be deleted by the Company immediately after the closure of the selection procedure.
If the Company would use the data of the given person in a procedure aimed at filling a position where judicial record should be submitted, the Company may request the given person to present again a valid judicial record.

Photocopying of personal identification card

In due consideration of the position of NAIH, the Company does not make photocopies of personal identification cards. A photocopy of an authoritative deed is not suitable for identifying natural persons in view of the fact that the presence of the person is inevitable for identifying him/her on the basis of such authoritative certificate. Obviously, a photo ID has probative force only in that case when on its basis the Company can ascertain that the person whose image is shown on the identification card and the person presenting such card are identical. A copy of an authoritative certificate has no probative force as regards the fact that it is a genuine copy of a valid authoritative certificate.

However, in order to observe principles related to data capturing and data quality, the Company may make a masked photocopy (or scanned image – together: photocopy) about the authenticating certificate of new recruits or employees modifying their data. In the course of photocopying, the Company will mask the identification card in such manner that only those parts will remain legible that the data subject is obliged to reveal in the course of joining the Company. In such case the photocopy is created for data reconciliation. The company will immediately and irrevocably erase or destroy a photocopy when the data shown on the masked photocopy of such personal identification card have been collated with the completed job application form by the designated member of the HR staff but latest within 30 days from the creation of the photocopy.

Processing health data related to medical fitness for work

Data related to the medical fitness of any of the data subjects will not be known and/or processed by the Company beyond the intended purpose. The company will pass its decision concerning the medical fitness of a given (prospective) employee for the work on the basis of the results of the relevant examination performed by the health care practitioner for the purpose of deciding fitness. The Company will process only those data that evidence medical fitness for work.
If in the course of the conclusion of employment contract it would be discovered that the given person is unfit for the job and therefore the employment relationship would not be established or would for this reason be terminated, the data processing deadlines and methods should be adjusted in parallel with that.

Disabled employees

From the aspect of data processing, identical rules are applicable for disabled workers than other employees of the Company, however, a larger scope of data are processed about them: see under the scope of data processed. (The Company controls health data of disabled workers on the basis of the provisions stipulated by the law.)

Data processing related to maintenance and termination of employment relationship

The Company keeps labour records about its employees. Payroll accounting is performed by the Company.

The Company stores the data of employees electronically and in hard copy. Those personal data of employees will be captured that are necessary for establishing employment relationship. The Company captures data electronically in its database.

The legal ground of controlling employees' data is statutory authorisation (Act I of 2012 on the Labour Code, and the consent of the data subject (Section 5 (1) a) and 6 (6) of Infotv.).

Data processing in respect of travels organised during the existence of employment relationship

The Company keeps a travel registry that contains those personal data of its employees, which are inevitably necessary for the organisation of travels in the interest of performance of tasks related to employment relationship during the existence of their employment relationship.

The Company organises travels in accordance with Sections 31 and 32 of KBT, in the frames of centralised public procurement process through the portal operated by the Directorate-General for Public Procurement and Supply (KEF) (address: 1119 Budapest, Andor u. 47-49) (utaztatas.kef.gov.hu: Portal operator: 1122 Budapest, Acsády I. u. 13), and in accordance with Section 15 (2) of Government Decree 168/2004 (V.25.), and in the interest of its streamlined arrangement, the Company is obliged to satisfy by deadline its data delivery and other obligations related to the submission of demands and orders. KEF utilises the services provided by the following travel agencies:
OTP Travel Kft. (1051 Budapest, Nádor u. 21.)
WECO Travel Kft. (1053 Budapest, Szép u. 2.)
IBUSZ Utazási Irodák Kft. (Budapest, Dayka G. u. 3.)

In the interest of complying with its data delivery obligation under the above legal rules and the streamlined arrangement of travels, the Company is obliged to furnish KEF with the following personal data regarding travellers: name, date of birth, citizenship, type, number, validity and the issuing authority of the personal identification card/passport.

Furthermore the Company, in the interest of the travellers, provides assistance in the arrangements for acquiring visa as necessary, and in this framework the co-workers dealing with travel organisation would contact the authorities or country representations issuing such visa in the interest of the persons concerned and transfer data for these organisations with the consent of the data subject.

The members of the staff engaged in travel organisation may process traveller-related actually valid digitised personal data that are necessary for travel arrangements within their scope of tasks exclusively in the interest of organising a travel, until the achievement of the aim of data processing but latest until the termination of the employment relationship. The members of the staff engaged in travel organisation are entitled to acquire traveller-related actually valid personal data from co-workers engaged in HR jobs, and such HR employees are entitled to furnish the members of the staff engaged in travel organisation with these data in the interest of measures to be taken for travel organisation.

The members of the Company's finance and controlling staff have access entitlement to the travel registry kept by the members of the staff engaged in travel organisation, exclusively until the compilation of the accounts.

In the frames of travel organisation activities, the legal ground of data processing performed by the Company is statutory authorisation [Sections 31 and 32 of Kbt., and Sections 10 (1) and (2) of Mt.] and the consent of the data subject [Sections 5 (1) and 6 (6) of Infotv.].

Declarations concerning data processing related to employment relationship

If in the interest of the establishment, maintenance and termination of employment relationship and for evidencing the relevant entitlements and/or in recognition of obligations, declarations should be obtained from the employees, in the course of obtaining such declarations, the Company in all cases notifies the employee on the fact, legal ground and purpose of processing data revealed in such declarations.

If the validity of a declaration is conditional upon the presentation of a deed (personal identification card, student card), the company will not handle the data of such deed and/or its photocopied or scanned image in any manner, but will certify the presentation and the validity of such deed by virtue of the signature affixed by its appropriately entitled employee.

Employee training

The Company reserves the right to conclude contract with a third party for the training of its employees. If such training would be statutorily binding for the given job, then such third party processes data as the Company's designated data processor; in the case of any other sort of training, the transfer of a personal data to a third party is conditional upon the consent of the employee. The tasks of the fire prevention and labour safety officer are performed by an external service provider.

purpose of data processing: establishment, maintenance or termination of employment relationship, recognition of the relevant eligibilities and certifying obligations

scope of processed data:

- photo,
- identification number,
- name,
- name at birth,
- place and date of birth,
- citizenship,
- mother's name at birth,
- address of the place of residence,
- place of stay (if it differs from the place of residence),
- private pension fund
  - membership,
  - date of admission (day, month, year),
  - bank's name and code,
- tax identification mark,
- social insurance identification mark (TAJ number),
- pensioner registration number (in the case of retired employee),
- copy of the labour booklet (if any)
- declaration on debts,
- declaration on the observation of data security rules,
- current bank account number,
- starting date of employment relationship,
- type of insurance legal relationship,
- weekly working hours,
- telephone number,
- marital status,
- copy of the deed certifying qualification,
- certificate of medical fitness for work,
- job,
- medical fitness and necessity of eye-glasses,
- judicial record
  - date of issue,
  - registration number,
  - identifier of the application,
- after termination of the employment relationship, a certificate of the performance of closing medical examination of fitness for the job,
- expert resolution grounding disability status in the case of a disabled employee,
- in the case of work performed besides the main employment relationship
  - nature of the legal relationship,
  - name and headquarters of the employer,
  - monthly average work time at the workplace besides the main employment relationship,
  - activity to be performed,

- certificates related to the previous employment relationship:
  - certificate of the insurance legal relationship and regarding health insurance benefit
  - certificate of the employer on the termination of employment relationship
  - tax basis for 2015
- regarding additional vacation due under Section 120 of Mt.
  - photocopy of the deed certifying the statement of disability in excess of fifty per cent issued by the rehabilitation experts organisation
  - photocopy of the deed certifying eligibility for disability subsidy,
  - photocopy of the deed certifying eligibility for benefits of the blind.

In the case of disabled employees on the basis of Sections 21, 21/A and 21/B of Act CXCI of 2011 on the benefits due for disabled persons and the amendment of certain Acts, the above scope of data is supplemented as follows:

- documents containing data related to the health status that under Section 3, point 3 of Infotv. qualify as special/sensitive personal data:
  - opinion of the expert committee (ORSZI – National Office of Rehabilitation and Social Affairs),
  - resolution on disability.

legal ground of data processing: statutory authorisation under Sections 10 (1) and (3) of Act I of 2012 on Labour Code, and the consent of the data subject [Sections 5 (1) a) and 6 (6) of Infotv.]
time scope of data storage: until the achievement of the intended purpose of data processing, according to the general rule:

- related to the rights and obligations under employment relationship: until the termination of the employment relationship
- regarding eligibilities stemming from the employment relationship: until the deadline determined in the legal rules on the payment of pension benefits.

method of data processing: in hard copies and electronically

***

Processing data of relatives in connection with employment relationship

In order to guarantee certain benefits, the Company processes data of the employees' relatives in connection with employment relationship. Data of third parties so obtained could be captured and processed not in excess of the necessary data content.

Such benefits can be the following: additional vacation, utilisation of family tax benefit, applying for subsidised travel pass qualifying as non-taxable in-kind benefit, and non-taxable school starting subsidy.

In the case when the employee submits the data of a third person, the employee is obliged to obtain the consent of such third person in order that the Company can certify that it is authorised to control the data of a third party.

purpose of data processing: to guarantee benefits in connection with employment relationship
scope of processed data: name, name at birth, place and date of birth, citizenship, mother's name at birth, residential address, tax identifier, TAJ number and contact data of the close relative of the employee
legal ground of data processing: consent of the data subject [Section 5 (1) a) of Infotv.]
time scope of data storage: until the achievement of the intended purpose of data processing, according to the general rule:

- related to the rights and obligations under employment relationship: until the termination of the employment relationship
- regarding eligibilities stemming from employment relationship: until the deadline determined in the legal rules on the payment of pension benefits

method of data processing: in hard copies and electronically

***

DATA PROCESSING IN CONNECTION WITH THE SURVEILLANCE OF THE TECHNICAL DEVICES EMPLOYEES

The employer may supervise the employees as regards their behaviour conducted in the context of the employment relationship. Such surveillance is legally grounded by Sections 11 (1) and (2) of Mt.

The Company notifies the employees in advance on the application of technical devices that serve for the surveillance of the employees.

In justified cases the Company furnishes employees with computer, company telephone, e-mail address and internet access for personal use. The Company informs employees on the rules of usage and the possibility of surveillance in a document titled Information Security Manual for Users.

purpose of data processing: in accordance with the lawful business interests of the Company, surveillance of employees under Section 11 (1) of Mt., specifically surveillance of the usage of computer, e-mail address, company telephone and internet access in the personal use of employees.
scope of processed data: personal data captured in the course of surveillance, specifically private e-mail addresses, private telephone numbers, photographs, personal computer documents, internet browsing history, cookies, the fact of perceiving any misdemeanour in the frames of employment relationship, description of the misdemeanour.
legal ground of data processing: Section 11 (1) of Act I of 2012 and occasionally Section 5 (1) a) of Act CXII of 2011.
time scope of data storage: one year from the surveillance, but latest the lapse of any demand stemming from the surveillance.
data storage method: electronically

***

SURVEILLANCE OF FITNESS FOR WORK FROM THE LABOUR SAFETY ASPECT

Section 52 (1) a) of Mt. states that employees are obliged to appear at the place and time specified by the employer in a condition fit for work.

On the basis of the authorisation ensured in Section 2 (3) of Mvt., as regards impairment by alcohol, the employer determines the requirements concerning health safe and secure work practices as follows:

In accordance with Section 60 (1) of Mvt. employees may perform work in a condition fit for the work, in due consideration of the rules and instructions related to labour safety, and in accordance with the labour safety training. The employee is obliged to cooperate with his/her colleagues and perform his/her work in such manner that therefore his/her own or anybody else's health or corporeal integrity would not be endangered.

In respect of each and every job the Company prohibits its employees from being present at the work premises under alcoholic influence – this should be applicable to those cases when the person concerned stays in the premises out of his/her working hours before/after working, in view of the fact that a person impaired by alcohol could endanger the safe work of others. It is prohibited to enter the premises of the

company or the company's work premises elsewhere, under the influence of alcohol, consume alcohol there, perform work under the influence of alcohol.

Exemption from this rule can be granted by the Senior Executive Officer in writing.

The conditions of secure work practices are endangered by unfitness for work, for instance impairment by alcohol. Therefore the persons concerned must be in a condition fit for work not only when appearing on the work premises but fitness for work must be maintained until the end of the work time.

In the course of performing work the employees may not endanger their own or anybody else's health or corporeal integrity.

By virtue of its obligation to arrange for the secure conditions of work practices, the Company is obliged to ascertain that employees observe the relevant prescriptions. Rules related to the surveillance of the observation of labour law prescriptions are described in more detail in Mt. as well as in Mvt.

Section 11 (1) of Mt: Employers shall be allowed to monitor the behaviour of workers only to the extent pertaining to the employment relationship. The employers' actions of control, and the means and methods used, may not be at the expense of human dignity. The private life of workers may not be violated.

Section 54 (7) b) of Mvt*.:* In the interest of occupational safety and health, employers shall observe the following general requirements: routinely review work conditions and ensure that they conform with requirements, and the workers have knowledge of and observe the provisions pertaining to them.

Surveillance of the observation of labour safety rules is the responsibility of the Company's Labour Safety Officer who could be appointed by the Senior Executive Officer of the Company in accordance with Section 57 (1) of Mvt. If he/she would be prevented from acting, the Labour Safety Officer may delegate the scope of surveillance authority to the security guards employed by the designated security services in accordance with Szvtv. Testing at the gatekeeper service may be performed exclusively by the members of the security staff.

However, testing of alcoholic impairment as described above may not entail the violation of the human dignity of employees – therefore the Labour Safety Officer may not abuse his/her surveillance authority, and may not exercise such right in contradiction with its intended purpose, for instance, if such surveillances are conducted several times a day without good reason or in retaliation; it is also unlawful if a person not vested with the appropriate scope of rights would require such testing.

Persons eligible to conduct tests:

- Senior Executive Officer,
- Labour Safety Officer,
- in the case when the Labour Safety Officer is prevented from acting: the Security Guard,
- in the case of tests at the gatekeeper service: the Security Guard.

The Labour Safety Officer may initiate tests with the random sampling method in accordance with his/her authorisation granted in Section 54 (7) b) of Mvt. Tests may be conducted by the Labour Safety Officer him/herself or may be delegated to the Security Guard.

The Security Guard may conduct such tests only in the case of actual suspicion and never with random sampling method.

The exact testing procedure:

- the Labour Safety Officer may at any time request the alcohol testing of any of the employees, even with the random sampling method,
- in the case of suspicion, the Line Manager of the person concerned is obliged to initiate proceedings,
- in response to notice from any of the employees of the Company, the Labour Safety Officer is entitled to request alcohol testing provided that the employees could indicate the reason for such testing and the person to be tested, however, the Labour Safety Officer is entitled to refuse such testing if the circumstances giving reason for measures do not suggest unambiguously that such testing would be justified,
- if the labour safety officer is prevented from acting, in response to notice from any of the employees of the Company, a security guard is also entitled to request alcohol testing provided that the employees could indicate the reason for such testing and the person to be tested, however, the security guard is entitled to refuse such testing if the circumstances giving reason for measures do not suggest unambiguously that such testing would be justified,
- employees should be tested without violating their personal right, in the presence of two witnesses either with alcohol sonde or with breathalyser,
- the person conducting such test should prepare a protocol, the protocol should contain the following: the fact of testing, the circumstance giving reason for testing (general purpose labour safety testing or suspicion of alcohol impairment), the person tested, time of testing, test result, legal declaration of the tested person regarding the result of the testing (accepts or does not accept),
- if an employee would not accept the result, he/she may initiate the checking of his/her blood alcohol level by taking blood sample,
- if an employee would not cooperate with the Labour Safety Officer and would not wish to undergo testing, the Labour Safety Officer should immediately notify the person who exercises employer's right over such employee,
- refusal of testing automatically qualifies as unfitness for working in accordance with Section 60 (1) of Mvt., because the employee refused his/her statutory cooperation obligation.

If the employee qualifies unfit for work (positive result or breaching of the cooperation obligation), the person conducting the test is obliged to immediately notify the person vested with employer's right or decision right over the employee who will then be obliged to exclude the employee from work.

If the test was conducted by the security guard on the basis of suspicion, as soon as the reason that prevented the Labour Safety Officer from acting would cease, the security guard is obliged to immediately notify the Labour Safety Officer on the test performed by him/her and its result.

purpose of data processing: check of fitness for work for labour safety purposes
scope of processed data: result of the test, time, fact of fitness for work, data of the person performing the test, data of the employee tested. If the tested person would debate the result, this fact; also, if the test was positive and the employee would abandon his/her right for blood test, this fact, too.
legal ground of data processing: Section 60 (1) of Act XCIII of 1993 on Labour Safety and Sections 11 (1) and (2) of Act I of 2012 on Labour Code.
time scope of data storage: the deadline open for enforcing claims grounded by the rights and obligations stemming from testing.
data storage method: in hard copies and electronically.

***

APPLICATION OF ELECTRONIC SURVEILLANCE SYSTEM

Please be informed that the Company applies closed circuit camera surveillance system in its site under 5 Budapesti Street, Szeged 6728.

The cameras form the Company's own property and are operated by the Company.

The camera records are stored on the local servers.

In the case of terror hazard the Constitution Protection Office may have access to the records in view of the fact that the site is a distinguished national security facility.

Sectors of the electronic surveillance system

The Company distinguishes the areas watched by the electronic surveillance system into two separate categories according to the aim of surveillance.
The first category is so-called Sector I where the legal rule that governs the applied electronic surveillance system is Section 31 (3) c) of Szvtv., because the aim of surveillance is the safe storage, handling and transportation of properties and equipments, money, securities, noble metal, precious stones that are of at least significant value as described in the Act on the Criminal Code.

The second category is the so-called Sector II where the legal rules that governs the applied electronic surveillance system is Section 31 (3) d) of Szvtv., because the aim of the surveillance is the safeguarding of hazardous materials.

Method of and deadline set for erasure of records generated by the electronic surveillance system

Sector I
As per Section 31 (3) c) of Szvtv. at the units specified by the Company, in the interest of the safe storage, handling and transportation of properties and equipments, money that are of at least significant value as described in the Act on the Criminal Code, records are stored for 30 days.

Sector II
As per Section 31 (3) d) of Szvtv., records taken in the interest of safeguarding hazardous materials are kept by the Company for 30 days.

In both cases the Company from among the rights that the data subjects are vested with guarantees those specified in Szvtv., i.e. if a record interferes with a person's rights or lawful interests, such person may within the deadline set for erasure as specified above (thirty days) request the data controller not to destroy and/or not to erase such record provided that he/she can certify his/her right or legal interest. The decision about such request will be passed by the internal Data Protection Officer of the Company within the shortest possible deadline. The record so distinguished should be saved and handed over to the internal Data Protection Officer who will arrange for its safeguarding in accordance with the data protection rules corresponding with this present Regulation. In response to any request from a court or other authority, the record should be sent to the court or authority without delay. If such request would not be received within thirty days from the day when the request for disregarding destruction was received, such record will be erased.

Warranty rules related to electronic surveillance

Through the electronic surveillance system, the Company interferes with the privacy of the data subject only to the necessary extent.

The Company does not apply electronic surveillance for whatever reason and in whatever manner in the following cases:

- surveillance of the work intensity of the employee,
- influencing the behaviour conducted by employees at the work premises,
- in sensitive areas, specifically changing room, shower, toilette,
- in areas where employees spend their relax time or breaks, specifically relaxation rooms, smoking areas,
- public areas.

However, the Company may apply electronic surveillance in order to gain confidence that the employees observe the regulations related to them in the interest of health safe and secure work practices.

Viewing images recorded by the cameras

In order that the Company would interfere with the privacy of the data subjects to the least extent, the images recorded by the electronic surveillance system may be accessed by designated persons only.

Within the organisational system of the Company, only the person designated in this present Regulation may view recorded images.

Blocking of camera images

Blocking of images taken by the cameras may be required only by a person designated to supervise data processing through the Company's camera system or the internal Data Protection Officer if he/she has been appointed.

Blocking of camera images may be initiated by:

- a person vested by the Company with right to view if in the course of viewing such images he/she would perceive any circumstance that would endanger the aim to be achieved by the electronic surveillance system,
- anybody, whose rights or lawful interests are interfered by the records.

Blocking of the camera records can be requested with an application addressed to the person designated to supervise data processing through the camera system and concurrently to the internal data protection officer if such person has been designated.

The decision about blocking will be passed by the person designated by the company for supervising data processing through the camera system within the shortest possible time (in agreement with the internal Data Protection Officer if such person has been designated).

The Company takes a protocol on blocking images recorded by the cameras, in which the time of viewing and blocking, its purpose furthermore the event giving reason for blocking and the indication of further use should be stated.

Persons vested with blocking eligibility

The Company keeps a registry on the scope of persons entitled to block images. Such registry contains the name and position of the person vested with blocking rights, date of issuing such blocking right, date of withdrawal of blocking right. The Company keeps such data for 5 years counted from withdrawal.

Sector I

purpose of data processing: storage, handling and transportation of properties, equipments and money qualifying as at least of significant value according to the Act on the Criminal Code

scope of processed data: portrait of the data subject, data that can be acquired with the camera image (place of stay, duration of stay),

legal ground of data processing: implied consent of the data subject [Section 30 (2) of Szvtv.]

time scope of data storage:

- if the record is not utilised, it will be erased within 30, say thirty days passing from recording [Section 31 (3) c) of Szvtv.]
- if following the certification of rights of lawful interests, the Company was requested not to destroy the record, meanwhile, request was not submitted, then the record will be erased within 30, say thirty days from such request [Section 31 (6) of Szvtv.]

method of data processing: electronically

Sector II

purpose of data processing: safeguarding hazardous materials

scope of processed data: portrait of the data subject, data that can be acquired with the camera image (place of stay, duration of stay),

legal ground of data processing: implied consent of the data subject [Section 30 (2) of Szvtv.]

- if the record is not utilised, it will be erased within 30, say thirty days from recording *[Section 31 (3) d) of Szvtv.]*
- if following the certification of rights of lawful interests, the Company was requested not to destroy the record, meanwhile, request was not submitted, then the record will be erased within 30, say thirty days passing from such request [Section 31 (6) of Szvtv.]

method of data processing: electronically

***

MANAGEMENT OF EXTRAORDINARY SECURITY EVENTS

Extraordinary event shall mean an event or circumstance that deviates from the average, which therefore may lead to severe consequences regarding life, corporeal integrity of persons staying in the facility or regarding properties to be found there, or there are realistic chances for leading to such consequences and therefore severe disturbance in the operation of the facility could be caused.

The Security Guards employed by the contracted service provider will take protocol on any event within the premises that is of relevance from the security aspect. Such protocol should contain the following data: date of taking protocol, name of the member of the staff of the security service, his/her signature, name of the person investigated, his/her signature, name at birth, place, date of birth, mother's name, residential address, place of stay of the person investigated and the description of the event. These data are relative personal data, therefore – under Infotv. – they might become personal data.

purpose of data processing: investigation of extraordinary security event

scope of processed data: date of capturing the protocol, name of the member of the staff of the security service, his/her signature, name of the person investigated, his/her signature, name at birth, place and time of birth, mother's name, residential address, place of stay of the person investigated and the description of the event

legal ground of data processing: consent of the data subject in accordance with Section 5 (1) a) of Infotv.

time scope of data storage: investigation of the event, the deadline available for enforcing claims regarding rights and obligations stemming therefrom.
data storage method: in hard copy

SECURITY SURVEILLANCES

In the interest of protecting properties, on the basis of the authorisation ensured by Section 26 of Szvtv., the Company conducts package, cabinet/locker, vehicle and cargo surveillance.

Such surveillance may be conducted by the Security Guard for the purpose of enforcing his/her obligations stemming from the contract, following notification as regards the reason and the aim of the measure, in those cases when

- it can be suspected with good ground that the person concerned keeps a thing acquired by criminal action or misdemeanour, and the safeguarding of such property is the contractual obligation of the Security Guard,
- such thing is not handed over despite the relevant request, and
- such measure is necessary for preventing or halting a law violating act.

If the surveillance is closed with tangible result, the Security Guard takes a protocol on the surveillance of the extraordinary event, and such protocol will be subjected to the relevant rules of data processing.

***

ACCESS CONTROL

Please be informed that in its plant located at 6728 Szeged, 5 Budapesti Street, the Company operates an electronic access control system. The plant is separated to several zones based on security and access eligibility aspects.

The green zone is the area that is open for clients; this area may be accessed by anyone without authentication of identity or any check.

The yellow zone is the area of the visitors' centre where visitors may enter following preliminary registration. After the authentication of the identity, the visitor will be provided with a badge. Registration will be executed in accordance with the provisions stipulated in the chapter about the visitors' centre.

Into the area of the orange zone exclusively employees and persons employed under other form of employment relationship may enter.

The red zone is intensely protected, it may be accessed by a narrow scope of employees (e.g. server room, security surveillance, etc.).

The black zone is the so-called laser space. This area may be accessed only by persons vested with distinguished access rights.

The white zone is a separated area where the kitchen can be found which is operated by an external firm.

Control of access by employees and persons employed under any other form of employment legal relationship

The rights to access premises of the Company vary with the individual jobs/positions.

Employees and persons employed under other form of employment relationship may move amongst the zones in correspondence with the eligibility levels shown on their entry card.

The card shows the name, card number and a photograph.

The access control system – and therefore the access control database – is operated by the Company. The entry data are stored on the Company's server.

purpose of data processing: security surveillance conducted in the course of controlling entrances and departures

scope of processed data: name, time of entrance/departure, identification number of the entering person

legal ground of data processing: consent of the data subject in accordance with Section 5 (1) a) of Infotv. and Section 32 of Act CXXXIII of 2005.

time scope of data storage:

- in the case of eligibility for regular entrances, the authentication data (name and identification number) necessary for the operation of the system will be deleted by the Company immediately after the termination of such eligibility,
- in the case of eligibility for regular entrances, those data that were generated in the course of the operation of the system will be deleted concurrently with the termination of such eligibility but latest after 6 months from the generation of such data.

data storage method: electronically

***

You may request information about the processing of your data, also, you may request the rectification of your personal data and erasure of those data – except for data processing requested by a legal rule – in the manner as indicated when your data have been captured and at the contact data indicated by the data controller.

Data controller

name:	ELI-HU Research and Development Non-profit Limited Liability Company
short name:	ELI-HU Non-profit Llc.
corporate registration number:	Cg.06-09-015211
headquarters:	6720 Szeged, 13 Dugonics Square
e-contact:	Info@eli-alps.hu
represented by:	Lóránt Ferenc Lehrner Managing Director

The entire data controlling system of ELI-HU Research and Development Non-profit Llc. is described in the Company's Data Protection Regulation.

The data subject may request legal remedy from and submit complaint to the National Authority of Data Protection and Freedom of Information (1125 Budapest, Szilágyi Erzsébet fasor 22/C.) or to the court of justice competent in the area of his/her place of residence or location.

DECLARATION MADE BY THE EMPLOYEE

Name of employee: .....

place and date of birth: .....

mother's name: .....

I have familiarised myself with the Data Protection Regulation of ELI-HU Research and Development Non-profit Llc. as well as the information material titled "Data protection information material for employees" forming Enclosure 5/1 of the former and hereby I give my consent to the data processing described therein.

....., ... 20.....

……..

signature

Enclosure No. 5/2

DATA PROTECTION INFORMATION MATERIAL FOR PERSONS EMPLOYED UNDER OTHER FORMS OF EMPLOYMENT RELATIONSHIP

Please be informed that in the frames of your employment legal relationship your personal data will be processed as follows:

Rules of data processing

In view of the fact that the right of informational self-determination is a fundamental right afforded by the Fundamental Law, in the course of any proceeding, the Company processes data only and exclusively on the basis of the provisions stipulated in the legal rules in force.

Personal data may exclusively be processed for a specific purpose to realize rights or fulfil obligations. The use of personal data in the control of the Company for private purposes is prohibited. Data controlling should always correspond with the purpose limitation principle.

Personal data may be processed by the Company to the minimum extent and for the shortest period necessary for the achievement of the specified and explicit purposes, where it is necessary for the implementation of certain rights and obligations. The purpose of processing must be satisfied in all stages of data processing operations, and in case the purpose of data processing has ceased or the data controlling otherwise violates the law, data should be erased. Erasure of data is the responsibility of the employee of the Company who actually processes such data. Erasure could be checked by the person actually exercising employer's rights over the employee and by the internal data protection officer – provided that such officer has been appointed or designated by the Company.

The Company may process personal data only on the basis of the preliminary consent of the data subject – in the case of special/sensitive personal data on the basis of written preliminary consent – or on the basis of legal rule or statutory authorisation.

Handling judicial records

In order to comply with the provisions stipulated in the legal rules and to meet commitments under other legal relationships, the Company reserves the right to hire researchers who comply with its moral expectations, therefore the Company may make the employment conditional upon clean judicial records.

Clean judicial record will be checked by the HR partner who will verify the:

- validity (in a manner available for anyone), and
- content of the judicial record.

The Company may handle personal data processed in criminal matters only with the written consent of the data subject. The Company preliminarily notifies the data subject about the reason for handling personal data processed in criminal matters, which is making a decision about data subject's worthiness for the given position; therefore such data will be handled until this purpose would be achieved, until the passing of the decision.

The Company requests clean criminal record as a condition for filling a given specific job. In cases deserving special consideration, the Company's Senior Executive Officer, in the course of individual evaluation may make positive decision concerning worthiness for a given job if according to the judicial record:

- the nature and severity of the act committed is not irreconcilable with the expectations related to the job to be filled,
- court exoneration is in progress,
- statutory exoneration is opportune,
- there are other reasons deserving special consideration which guarantee that the Company's mission and principles would be not endangered.

In the course of aspiring for a job, data are transferred to the person vested with decision right on the ground discussed hereunder. The evaluation of the aptitude for the job is the responsibility of 3 researcher experts and the HR expert. Data given in the course of application for a job could therefore be known not only by these 3 researcher experts and the HR Expert, but – in the special case described above – by the Senior Executive Officer of the Company, too.

The data may not be known by others than those indicated above, therefore other employees of the Company or any other person having legal relationship with the Company may not have access to such data in any manner or form.

In the course of the establishment of other form employment legal relationship in respect of a given scope of tasks, the data subject submits his/her valid judicial record. In view of the fact that the worthiness for the job is decided by the 3 researcher experts and the HR Expert, all of the data must be transferred to them. However, the Company in all cases seeks the best method for not restricting the privacy of the data subject and in consideration of the fact that a valid judicial record may within 90 days from its issue be used for purposes other than applying for a job with the Company, the Company physically does not file the judicial record of the data subject.

In order to achieve that data shown on the judicial record could be accessed only by the competent person, the Company obligatorily requests that in the course of the recruitment procedure the judicial record could be revealed by the applicant only for the 3 researcher experts and the HR Expert and – in the special case described in this present point – for the Company's Senior Executive Officer.

In the cases deserving special consideration, if in the course of the procedure aimed at the establishment of employment relationship, the data subject cannot present his/her judicial record, such judicial record may be mailed to the company in order to make documentation complete. In such case within a deadline of 30 days

- the Professional Manager makes decision on other form of employment legal relationship,
- the document will after the closure of the decision process be successively sent back to the data subject in a traceable manner.

In order that the Company could prove

- that in the course of the recruitment process, it has inspected the validity of the judicial record,
- what sort of available data were used for the evaluation of the prospective employee in the course of the recruitment process,
  together with the data necessary for the maintenance of the employment relationship, the following data will also be captured in the same manner and with the same storage deadline:
  - date of issue of the judicial record
  - deed number of the judicial record
  - identifier of the application for judicial record.

However, according to the legal rules these data do not qualify as special/sensitive personal data because they are not personal data processed in criminal matters. On the basis of the data mentioned above, the

genuineness and the content of judicial records issued after 1 January 2013 can be successively verified in the system of KEKKH.

Therefore the Company does not store any judicial record either in the course of the recruitment procedure or during the employment relationship and does not make copy of the judicial record.

In the event when a given applicant would not be selected, his/her data i.e. data related to his/her judicial records will be deleted by the Company immediately after the closure of the selection procedure.

If the Company would use the data of the given person in a procedure aimed at filling a position where judicial record should be submitted, the Company may request the given person to present again a valid judicial record.

Photocopying of personal identification card

In due consideration of the position of NAIH, the Company does not make photocopies of personal identification cards. A photocopy of an authoritative deed is not suitable for identifying natural persons in view of the fact that the presence of the person is inevitable for identifying him/her on the basis of such authoritative certificate. Obviously, a photo ID has probative force only in that case when on its basis the Company can ascertain that the person whose image is shown on the identification card and the person presenting such card are identical. A copy of an authoritative certificate has no probative force as regards the fact that it is a genuine copy of a valid authoritative certificate.

However, in order to observe principles related to data capturing and data quality, the Company may make a masked photocopy (or scanned image – together: photocopy) about the authenticating certificate of persons employed under other form of employment relationship who are newly recruited or who have modified their data. In the course of photocopying, the Company will mask the identification card in such manner that only those parts will remain legible that the person employed under other form of employment relationship is obliged to reveal in the course of joining the Company. In such case the photocopy is created for data reconciliation. The company will immediately and irrevocably erase or destroy a photocopy when the data shown on the masked photocopy of such personal identification card have been collated with the completed job application form by the designated member of the HR staff but latest within 30 days from the creation of the photocopy.

Processing health data related to medical fitness for work

Data related to the medical fitness of any of the data subjects will not be known and/or processed by the Company beyond the intended purpose. The company will pass its decision concerning the medical fitness for the work of a given person (to be) employed under other form of employment legal relationship, on the basis of the results of the relevant examination performed by the health care practitioner for the purpose of deciding fitness. The Company will process only those data that evidence medical fitness for work.
If in the course of the conclusion of the contract it would be discovered that the given person is unfit for the scope of tasks and therefore such other employment legal relationship would not be established or would for this reason be terminated, the data processing deadlines and methods should be adjusted in parallel with that.

Data processing in respect of travel organisation

The Company keeps a travel registry containing those personal data of persons employed under other form of employment legal relationship, which are inevitably necessary for the organisation of travels in the interest of performance of tasks related to their legal relationship.

The Company organises travels in accordance with Sections 31 and 32 of KBT, in the frames of centralised public procurement process through the portal operated by the Directorate-General for Public Procurement and Supply (KEF) (address: 1119 Budapest, Andor u. 47-49) (utaztatas.kef.gov.hu: Portal operator: 1122 Budapest, Acsády I. u. 13), and in accordance with Section 15 (2) of Government Decree 168/2004 (V.25.), and in the interest of its streamlined arrangement, the Company is obliged to satisfy by deadline its data delivery and other obligations related to the submission of demands and orders. KEF utilises the services provided by the following travel agencies:
OTP Travel Kft. (1051 Budapest, Nádor u. 21.)
WECO Travel Kft. (1053 Budapest, Szép u. 2.)
IBUSZ Utazási Irodák Kft. (Budapest, Dayka G. u. 3.)

In the interest of complying with its data delivery obligation under the above legal rules and the streamlined arrangement of travels, the Company is obliged to furnish KEF with the following personal data regarding travellers: name, date of birth, citizenship, type, number, validity and the issuing authority of the personal identification card/passport.

Furthermore the Company, in the interest of the travellers, provides assistance in the arrangements for acquiring visa as necessary, and in this framework the co-workers dealing with travel organisation would contact the authorities or country representations issuing such visa in the interest of the persons concerned and transfer data for these organisations with the consent of the data subject.

The members of the staff engaged in travel organisation may process traveller-related actually valid digitised personal data that are necessary for travel arrangements within their scope of tasks exclusively in the interest of organising a travel, until the achievement of the aim of data processing but latest until the termination of the employment relationship. The members of the staff engaged in travel organisation are entitled to acquire traveller-related actually valid personal data from co-workers engaged in HR jobs, and such HR employees are entitled to furnish the members of the staff engaged in travel organisation with these data in the interest of measures to be taken for travel organisation.

In the frames of travel organisation activities, the legal ground of data processing performed by the Company is statutory authorisation [Sections 31 and 32 of Kbt.] and the consent of the data subject [Sections 5 (1) and 6 (6) of Infotv.].

As regards the processing of personal data of persons employed under other form of employment legal relationship (researchers), an information material has been elaborated with the aim of providing the data subjects with preliminary information on data processing, which is attached as Enclosure 5/2 to this regulation.

purpose of data processing: establishment or termination of employment under other employment legal relationship, recognition of the related eligibilities and certification of obligations

scope of processed data: the data subject's

- photo,
- identification number,
- name,
- name at birth,
- place and date of birth,
- citizenship,
- mother’s name at birth,
- address of the place of residence,
- place of stay (if it differs from the place of residence),
- tax identification mark,

- tax number
- social insurance identification mark (TAJ number),
- current account number,
- starting date of the employment under other employment relationship,
- telephone number,
- job,
- medical fitness and necessity of eye-glasses,
- judicial record
  - date of issue,
  - registration number,
  - identifier of the application,

legal ground of data processing: consent of the data subject [Sections 5 (1) a) and 6 (6) of Infotv.]

time scope of data storage: until the achievement of the intended purpose of data processing , according to the general rule:

- related to the rights and obligations of persons employed under any other form of employment legal relationship: until the termination of the legal relationship,
- regarding eligibilities stemming from other form of employment legal relationship: until the deadline determined in the legal rules on the payment of pension benefits.

method of data processing: in hard copies and electronically

***

DATA PROCESSING IN CONNECTION WITH THE SURVEILLANCE OF THE TECHNICAL DEVICES PERSONS EMPLOYED UNDER OTHER FORM OF EMPLOYMENT LEGAL RELATIONSHIP

The Company may supervise data subjects as regards their behaviour conducted in the frames of their other employment legal relationship. Such surveillance is legally grounded by Sections 11 (1) and (2) of Mt.

Persons employed under other form of employment legal relationship are notified by the Company in advance on the application of technical devices that serve for the surveillance of the employees.

The Company furnishes persons employed under other forms of employment legal relationship with computer, company telephone, e-mail address and internet access for personal use. The Company informs data subjects on the rules of usage and the possibility of surveillance in a document titled Information Security Manual for Users.

purpose of data processing: in accordance with the lawful business interests of the Company, surveillance of persons employed under any other form of employment relationship, in accordance with Section 11 (1) of Mt., specifically surveillance of the usage of computer, e-mail address, company telephone and internet access in the personal use of persons employed under any other form of employment relationship.
scope of processed data: personal data captured in the course of surveillance, specifically private e-mail addresses, private telephone numbers, photographs, personal computer documents, internet browsing history, cookies, the fact of perceiving any misdemeanour in the frames of employment relationship, description of the misdemeanour.
legal ground of data processing: Section 11 (1) of Act I of 2012 and occasionally Section 5 (1) a) of Act CXII of 2011

time scope of data storage: one year from the surveillance, but latest the lapse of any demand stemming from the surveillance
data storage method: electronically

***

SURVEILLANCE OF FITNESS FOR WORK FROM THE LABOUR SAFETY ASPECT

Section 52 (1) a) of Mt. states that employees and persons employed under any other form of employment legal relationship are obliged to appear at the place and time specified by the employer in a condition fit for work.

On the basis of the authorisation ensured in Section 2 (3) of Mvt., as regards impairment by alcohol, the employer determines the requirements concerning health safe and secure work practices as follows:

In accordance with Section 60 (1) of Mvt. employees and persons employed under any other form of employment legal relationship may perform work in a condition fit for the work, in due consideration of the rules and instructions related to labour safety, and in accordance with the labour safety training. The employee is obliged to cooperate with his/her colleagues and perform his/her work in such manner that therefore his/her own or anybody else's health or corporeal integrity would not be endangered.

In respect of each and every job the Company prohibits its employees and other persons employed under any other form of employment legal relationship from being present at the work premises under alcoholic influence – this should be applicable to those cases when the person concerned stays in the premises out of his/her working hours before/after working, in view of the fact that a person impaired by alcohol could endanger the safe work of others. It is prohibited to enter the premises of the company or the company's work premises elsewhere, under the influence of alcohol, consume alcohol there, perform work under the influence of alcohol.

Exemption from this rule can be granted by the Senior Executive Officer in writing.

The conditions of secure work practices are endangered by unfitness for work, for instance impairment by alcohol. Therefore the persons concerned must be in a condition fit for work not only when appearing on the work premises but fitness for work must be maintained until the end of the work time.

In the course of performing work, employees and persons employed under any other form of employment legal relationship may not endanger their own or anybody else's health or corporeal integrity.

By virtue of its obligation to arrange for the secure conditions of work practices, the Company is obliged to ascertain that employees and persons employed under any other form of employment legal relationship observe the relevant prescriptions. Rules related to the surveillance of the observation of labour law prescriptions are described in more detail in Mt. as well as in Mvt.

Section 54 (7) b) of Mvt.: In the interest of occupational safety and health, employers shall observe the following general requirements: routinely review work conditions and ensure that they conform with requirements, and the workers and other persons employed in legal work performance relationship have knowledge of and observe the provisions pertaining to them.

Surveillance of the observation of labour safety rules is the responsibility of the Company's Labour Safety Officer who could be appointed by the Senior Executive Officer of the Company in accordance with Section 57 (1) of Mvt. If he/she would be prevented from acting, the Labour Safety Officer may delegate the scope of surveillance authority to the security guards employed by the designated security services in

accordance with Szvtv. Testing at the gatekeeper service may be performed exclusively by the members of the security staff.

However, testing of alcoholic impairment as described above may not entail the violation of the human dignity of employees and persons employed under any other form of employment legal relationship – therefore the Labour Safety Officer may not abuse his/her surveillance authority, and may not exercise such right in contradiction with its intended purpose, for instance, if such surveillances are conducted several times a day without good reason or in retaliation; it is also unlawful if a person not vested with the appropriate scope of rights would require such testing.

Persons eligible to conduct tests:

- Senior Executive Officer,
- Labour Safety Officer,
- in the case when the Labour Safety Officer is prevented from acting: the Security Guard,
- in the case of tests at the gatekeeper service: the Security Guard.

The Labour Safety Officer may initiate tests with the random sampling method in accordance with his/her authorisation granted in Section 54 (7) b) of Mvt. Tests may be conducted by the Labour Safety Officer him/herself or may be delegated to the Security Guard.

The Security Guard may conduct such tests only in the case of actual suspicion and never with random sampling method.

The exact testing procedure:

- the Labour Safety Officer may at any time request the alcohol testing of any of the employees or other persons employed under any other form of employment legal relationship, even with the random sampling method,
- in the case of suspicion, the Line Manager of the person concerned is obliged to initiate proceedings,
- in response to notice from any of the employees of or persons employed under any other form of employment legal relationship by the Company, the Labour Safety Officer is entitled to request alcohol testing provided that the employees and persons employed under any other form of employment legal relationship could indicate the reason for such testing and the person to be tested, however, the Labour Safety Officer is entitled to refuse such testing if the circumstances giving reason for measures do not suggest unambiguously that such testing would be justified,
- if the labour safety officer is prevented from acting, in response to notice from any of the employees of or persons employed under any other form of employment legal relationship by the Company, a security guard is also entitled to request alcohol testing provided that the employees and persons employed under any other form of employment legal relationship could indicate the reason for such testing and the person to be tested, however, the security guard is entitled to refuse such testing if the circumstances giving reason for measures do not suggest unambiguously that such testing would be justified,
- employees and persons employed under any other form of employment legal relationship should be tested without violating their personal right, in the presence of two witnesses either with alcohol sonde or with breathalyser,
- the person conducting such test should prepare a protocol, the protocol should contain the following: the fact of testing, the circumstance giving reason for testing (general purpose labour safety testing or suspicion of alcohol impairment), the person tested, time of testing, test result, legal declaration of the tested person regarding the result of the testing (accepts or does not accept),

- if an employee or a person employed under any other form of employment legal relationship would not accept the result, he/she may initiate the checking of his/her blood alcohol level by taking blood sample,
- if an employee or a person employed under any other form of employment legal relationship would not cooperate with the Labour Safety Officer and would not wish to undergo testing, the Labour Safety Officer should immediately notify the person who exercises employer's right over such employee,
- refusal of testing automatically qualifies as unfitness for working in accordance with Section 60 (1) of Mvt., because the employee refused his/her statutory cooperation obligation.

If the employee or person employed under any other form of employment legal relationship qualifies unfit for work (positive result or breaching of the cooperation obligation), the person conducting the test is obliged to immediately notify the person vested with employer's right or decision right over the employee or person employed under any other form of employment legal relationship who will then be obliged to exclude the employee or persons employed under any other form of employment legal relationship from work.

If the test was conducted by the security guard on the basis of suspicion, as soon as the reason that prevented the Labour Safety Officer from acting would cease, the security guard is obliged to immediately notify the Labour Safety Officer on the test performed by him/her and its result.

scope of processed data: result of the test, time, fact of fitness for work, data of the person performing the test, data of the employee or the person employed under any other form of employment legal relationship tested. If the tested person would debate the result, this fact; also, if the test was positive and the employee or persons employed under any other form of employment legal relationship would abandon his/her right for blood test, this fact, too.
legal ground of data processing: Section 60 (1) of Act XCIII of 1993 on Labour Safety and Sections 11 (1) and (2) of Act I of 2012 on Labour Code.
time scope of data storage: the deadline open for enforcing claims grounded by the rights and obligations stemming from testing.
data storage method: in hard copies and electronically.

***

PUBLICATION OF SCIENTIFIC ARTICLES

Scientific articles and results elaborated by researchers may be published by the Company under the name of the Company, for three months counted from the elaboration of the results.

APPLICATION OF ELECTRONIC SURVEILLANCE SYSTEM

Please be informed that the Company applies closed circuit camera surveillance system in its site under 5 Budapesti Street, Szeged 6728.

The cameras form the Company's own property and are operated by the Company.

The camera records are stored on the local servers.

In the case of terror hazard the Constitution Protection Office may have access to the records in view of the fact that the site is a distinguished national security facility.

Sectors of the electronic surveillance system

The Company distinguishes the areas watched by the electronic surveillance system into two separate categories according to the aim of surveillance.
The first category is so-called Sector I where the legal rule that governs the applied electronic surveillance system is Section 31 (3) c) of Szvtv., because the aim of surveillance is the safe storage, handling and transportation of properties and equipments, money, securities, noble metal, precious stones that are of at least significant value as described in the Act on the Criminal Code.

The second category is the so-called Sector II where the legal rules that governs the applied electronic surveillance system is Section 31 (3) d) of Szvtv., because the aim of the surveillance is the safeguarding of hazardous materials.

Method of and deadline set for erasure of records generated by the electronic surveillance system

Sector I
As per Section 31 (3) c) of Szvtv. at the units specified by the Company, in the interest of the safe storage, handling and transportation of properties and equipments, money that are of at least significant value as described in the Act on the Criminal Code, records are stored for 30 days.

Sector II
As per Section 31 (3) d) of Szvtv., records taken in the interest of safeguarding hazardous materials are kept by the Company for 30 days.

In both cases the Company from among the rights that the data subjects are vested with guarantees those specified in Szvtv., i.e. if a record interferes with a person's rights or lawful interests, such person may within the deadline set for erasure as specified above (thirty days) request the data controller not to destroy and/or not to erase such record provided that he/she can certify his/her right or legal interest. The decision about such request will be passed by the internal Data Protection Officer of the Company within the shortest possible deadline. The record so distinguished should be saved and handed over to the internal Data Protection Officer who will arrange for its safeguarding in accordance with the data protection rules corresponding with this present Regulation. In response to any request from a court or other authority, the record should be sent to the court or authority without delay. If such request would not be received within thirty days from the day when the request for disregarding destruction was received, such record will be erased.

Warranty rules related to electronic surveillance

Through the electronic surveillance system, the Company interferes with the privacy of the data subject only to the necessary extent.

The Company does not apply electronic surveillance for whatever reason and in whatever manner in the following cases:

- surveillance of the work intensity of the employee,
- influencing the behaviour conducted by employees at the work premises,
- in sensitive areas, specifically changing room, shower, toilette,
- in areas where employees spend their relax time or breaks, specifically relaxation rooms, smoking areas,
- public areas.

However, the Company may apply electronic surveillance in order to gain confidence that the employees observe the regulations related to them in the interest of health safe and secure work practices.

Viewing images recorded by the cameras

In order that the Company would interfere with the privacy of the data subjects to the least extent, the images recorded by the electronic surveillance system may be accessed by designated persons only.

Within the organisational system of the Company, only the person designated in this present Regulation may view recorded images.

Blocking of camera images

Blocking of images taken by the cameras may be required only by a person designated to supervise data processing through the Company's camera system or the internal Data Protection Officer if he/she has been appointed.

Blocking of camera images may be initiated by:

- a person vested by the Company with right to view if in the course of viewing such images he/she would perceive any circumstance that would endanger the aim to be achieved by the electronic surveillance system,
- anybody, whose rights or lawful interests are interfered by the records.

Blocking of the camera records can be requested with an application addressed to the person designated to supervise data processing through the camera system and concurrently to the internal data protection officer if such person has been designated.

The decision about blocking will be passed by the person designated by the company for supervising data processing through the camera system within the shortest possible time (in agreement with the internal Data Protection Officer if such person has been designated).

The Company takes a protocol on blocking images recorded by the cameras, in which the time of viewing and blocking, its purpose furthermore the event giving reason for blocking and the indication of further use should be stated.

Persons vested with blocking eligibility

The Company keeps a registry on the scope of persons entitled to block images. Such registry contains the name and position of the person vested with blocking rights, date of issuing such blocking right, date of withdrawal of blocking right. The Company keeps such data for 5 years counted from withdrawal.

Sector I

purpose of data processing: storage, handling and transportation of properties, equipments and money qualifying as at least of significant value according to the Act on the Criminal Code

scope of processed data: portrait of the data subject, data that can be acquired with the camera image (place of stay, duration of stay),

legal ground of data processing: implied consent of the data subject [Section 30 (2) of Szvtv.]

time scope of data storage:

- if the record is not utilised, it will be erased within 30, say thirty days passing from recording [Section 31 (3) c) of Szvtv.]

- if following the certification of rights of lawful interests, the Company was requested not to destroy the record, meanwhile, request was not submitted, then the record will be erased within 30, say thirty days from such request [Section 31 (6) of Szvtv.]

method of data processing: electronically

Sector II

purpose of data processing: safeguarding hazardous materials

scope of processed data: portrait of the data subject, data that can be acquired with the camera image (place of stay, duration of stay),

legal ground of data processing: implied consent of the data subject [Section 30 (2) of Szvtv.]

- if the record is not utilised, it will be erased within 30, say thirty days from recording *[Section 31 (3) d) of Szvtv.]*
- if following the certification of rights of lawful interests, the Company was requested not to destroy the record, meanwhile, request was not submitted, then the record will be erased within 30, say thirty days passing from such request [Section 31 (6) of Szvtv.]

method of data processing: electronically

***

MANAGEMENT OF EXTRAORDINARY SECURITY EVENTS

Extraordinary event shall mean an event or circumstance that deviates from the average, which therefore may lead to severe consequences regarding life, corporeal integrity of persons staying in the facility or regarding properties to be found there, or there are realistic chances for leading to such consequences and therefore severe disturbance in the operation of the facility could be caused.

The Security Guards employed by the contracted service provider will take protocol on any event within the premises that is of relevance from the security aspect. Such protocol should contain the following data: date of taking protocol, name of the member of the staff of the security service, his/her signature, name of the person investigated, his/her signature, name at birth, place, date of birth, mother's name, residential address, place of stay of the person investigated and the description of the event. These data are relative personal data, therefore – under Infotv. – they might become personal data.

purpose of data processing: investigation of extraordinary security event

scope of processed data: date of capturing the protocol, name of the member of the staff of the security service, his/her signature, name of the person investigated, his/her signature, name at birth, place and time of birth, mother's name, residential address, place of stay of the person investigated and the description of the event

legal ground of data processing: consent of the data subject in accordance with Section 5 (1) a) of Infotv.

time scope of data storage: investigation of the event, the deadline available for enforcing claims regarding rights and obligations stemming therefrom.

data storage method: in hard copy

SECURITY SURVEILLANCES

In the interest of protecting properties, on the basis of the authorisation ensured by Section 26 of Szvtv., the Company conducts package, cabinet/locker, vehicle and cargo surveillance.

Such surveillance may be conducted by the Security Guard for the purpose of enforcing his/her obligations stemming from the contract, following notification as regards the reason and the aim of the measure, in those cases when

- it can be suspected with good ground that the person concerned keeps a thing acquired by criminal action or misdemeanour, and the safeguarding of such property is the contractual obligation of the Security Guard,
- such thing is not handed over despite the relevant request, and
- such measure is necessary for preventing or halting a law violating act.

If the surveillance is closed with tangible result, the Security Guard takes a protocol on the surveillance of the extraordinary event, and such protocol will be subjected to the relevant rules of data processing.

***

ACCESS CONTROL

Please be informed that in its plant located at 6728 Szeged, 5 Budapesti Street, the Company operates an electronic access control system. The plant is separated to several zones based on security and access eligibility aspects.

The green zone is the area that is open for clients; this area may be accessed by anyone without authentication of identity or any check.

The yellow zone is the area of the visitors' centre where visitors may enter following preliminary registration. After the authentication of the identity, the visitor will be provided with a badge. Registration will be executed in accordance with the provisions stipulated in the chapter about the visitors' centre.

Into the area of the orange zone exclusively employees and persons employed under other form of employment relationship may enter.

The red zone is intensely protected, it may be accessed by a narrow scope of employees (e.g. server room, security surveillance, etc.).

The black zone is the so-called laser space. This area may be accessed only by persons vested with distinguished access rights.

The white zone is a separated area where the kitchen can be found which is operated by an external firm.

Control of access by employees and persons employed under any other form of employment legal relationship

The rights to access premises of the Company vary with the individual jobs/positions.

Employees and persons employed under other form of employment relationship may move amongst the zones in correspondence with the eligibility levels shown on their entry card.

The card shows the name, card number and a photograph.

The access control system – and therefore the access control database – is operated by the Company. The entry data are stored on the Company's server.

purpose of data processing: security surveillance conducted in the course of controlling entrances and departures

scope of processed data: name, time of entrance/departure, identification number of the entering person

legal ground of data processing: consent of the data subject in accordance with Section 5 (1) a) of Infotv. and Section 32 of Act CXXXIII of 2005.

time scope of data storage:

- in the case of eligibility for regular entrances, the authentication data (name and identification number) necessary for the operation of the system will be deleted by the Company immediately after the termination of such eligibility,
- in the case of eligibility for regular entrances, those data that were generated in the course of the operation of the system will be deleted concurrently with the termination of such eligibility but latest after 6 months from the generation of such data.

data storage method: electronically

***

You may request information about the processing of your data, also, you may request the rectification of your personal data and erasure of those data – except for data processing requested by a legal rule – in the manner as indicated when your data have been captured and at the contact data indicated by the data controller.

Data controller

name:	ELI-HU Research and Development Non-profit Limited Liability Company
short name:	ELI-HU Non-profit Llc.
corporate registration number:	Cg.06-09-015211
headquarters:	6720 Szeged, 13 Dugonics Square
e-contact:	Info@eli-alps.hu
represented by:	Lóránt Ferenc Lehrner Managing Director

The entire data controlling system of ELI-HU Research and Development Non-profit Llc. is described in the Company's Data Protection Regulation.

The data subject may request legal remedy from and submit complaint to the National Authority of Data Protection and Freedom of Information (1125 Budapest, Szilágyi Erzsébet fasor 22/C.) or to the court of justice competent in the area of his/her place of residence or location.

DECLARATION

Person employed under other form of employment legal relationship

Name of employee: .....

place and date of birth: .....

mother's name: .....

I have familiarised myself with the Data Protection Regulation of ELI-HU Research and Development Non-profit Llc. as well as the information material titled "Data protection information material for persons employed under other form of employment legal relationship " forming Enclosure 5/2 of the former and hereby I give my consent to the data processing described therein.

....., ... 20.....

.....

signature

Enclosure No. 5/3

DATA PROTECTION INFORMATION TO BE INSERTED INTO APPLICATION FOR TRAVEL

"The data protection regulation forms inseparable part of this present travel application, the content of which I am aware of and deem that to be binding for me, and hereby I am giving my consent to the processing and transferring of my personal data necessary for travel organisation."

Enclosure No. 6

DECLARATION OF RELATIVES REGARDING DATA PROCESSING

Employee	
Name:	
Job:	

Close relative	
Degree of relationship with the employee:	
Name: [1] [2] [3]	
Place and date of birth: [1]	
Mother's name: [1]	
Tax identifier (if any): [1] [2]	
Residential address: [1]	
Contact data: [3]	
By virtue of my signature hereby I am giving my consent to ELI-HU Research and Development Non-profit Llc. to process my data in order to ensure benefits related to my employment relationship.	
Date:	
Signature: [4]	

[1] In the case of family tax benefit to be completed about the child.
[2] To be completed in the case of family tax benefit provided that such family tax benefit is distributed among the members.
[3] In the case of personal accident the name of the person to be notified.
[4] In the case of person under the age of 16, signature of the legal representative

In the context of the employment relationship, the Company processes the data of the relatives of the employees in the interest of enforcing benefits. Such benefits could be additional vacation, utilisation of family tax benefit, tax-free school starting subsidy or eventually the registration of a person to be notified following a personal accident in order to facilitate quick communication. By virtue of completing this declaration, the relative gives his/her consent to data processing.

Enclosure No. 7/1

DATA PROTECTION INFORMATION FOR VISITORS OF THE VISITOR'S CENTRE

Data controller

name:	ELI-HU Research and Development Non-profit Limited Liability Company
short name:	ELI-HU Non-profit Llc.
corporate registration number:	Cg.06-09-015211
headquarters:	6720 Szeged, 13 Dugonics Square
e-contact:	Info@eli-alps.hu
represented by:	Lóránt Ferenc Lehrner Managing Director

Please be informed, that in the context of your visit to the research centre, your personal data are processed as follows:

purpose of data processing: enabling visits to the research centre

scope of data processed: name, date of birth and place of birth, mother's name

legal ground of data processing: consent of the data subject given in accordance with Section 5 (1) a) of Act CXII of 2011

time scope of data storage: until the achievement of the intended purpose of data processing but at most one year

data storage method: electronically and in hard copies

The research centre may be visited after preliminary notice and registration.

Preliminary application should be submitted 168 hours prior to the visit.

Applications can be submitted through an electronic interface by way of completing data shown in Enclosure 7/3 and furthering the completed document to the following e-mail address: pr@eli-alps.hu.

Preliminary registration is necessary in order to meet the obligation to cooperate with authorities.

Keeping contact with the Constitution Protection Office is prescribed in Section 28 (3) of Act CXXV of 1995 on National Security Services (hereinafter: Nbtv.).

In the course of applying for visit, the following data should be given: name, date of birth and place of birth, mother's name.

The transferred data will be processed by the unit responsible for Security Surveillance.

Personal data captured will be transferred to the Constitution Protection Office which is appropriately authorised by a specific legal rule (Nbtv.) in view of the fact that the research centre qualifies as a facility to be protected for national security reasons according to Government Decree 2009/2015 (XII.29.).

In view of the fact that the right of informational self-determination is a fundamental right afforded by the Fundamental Law, in the course of any proceeding, the Company processes data only and exclusively on the basis of the provisions stipulated in the legal rules in force.

Personal data may exclusively be processed for a specific purpose to realize rights or fulfil obligations. The use of personal data in the control of the Company for private purposes is prohibited. Data controlling should always correspond with the purpose limitation principle.

Personal data may be processed by the Company to the minimum extent and for the shortest period necessary for the achievement of the specified and explicit purposes, where it is necessary for the implementation of certain rights and obligations. The purpose of processing must be satisfied in all stages of data processing operations, and in case the purpose of data processing has ceased or the data controlling otherwise violates the law, data should be erased. Erasure of data is the responsibility of the employee of the Company who actually processes such data. Erasure could be checked by the person actually exercising employer's rights over the employee and by the internal data protection officer – provided that such officer has been appointed or designated by the Company.

The Company may process personal data only on the basis of the preliminary consent of the data subject – in the case of special/sensitive personal data on the basis of written preliminary consent – or on the basis of legal rule or statutory authorisation.

Prior to capturing a data, the Company in all cases informs the data subject about the purpose and the legal ground of data processing.

The Company does not engage data processor in the operation of the visitor's centre.

Enforcement of the rights of data subjects

A data subject may request information about the processing of his/her personal data, furthermore he/she may request the rectification of his/her personal data or its erasure – except if data processing is regulated by legal rules – such requests should be addressed to the contact possibilities of the Company.

The Company is obliged to transfer such request or objection within three days from its receipt to the Head of the Organisational Unit that is vested with responsibility and authority regarding data processing.

The Head of the Organisational Unit vested with responsibility and authority should give a properly understandable answer to the request regarding the processing of the data of the data subject, latest within 25 – in the case when right to object was exercised within 15 – days in writing from the receipt of the request/objection.

Such notification should cover the information specified in Section 15 (1) of Infotv. if the notification of the person concerned may not be refused under the said Act.

The notification in general is free of charge, the Company charges reimbursable costs only in the case specified in Section 15 (5) of Infotv.

The Company refuses any application only for reasons specified in Sections 9 (1) or 19 of Infotv., which should be justified in accordance with Section 16 (2) of Infotv. in writing.

The Head of the Organisational Unit that processes data will rectify untrue data provided that the necessary data and the evidencing public deeds are available, furthermore, if causes specified in Section 17 (2) of Infotv. would prevail, he/she takes measures for the erasure of the processed personal data.

For the period necessary for the evaluation of the objection submitted by the data subject against the processing of his/her data – but at most for 5 days – the Head of the Organisational Unit responsible for

data processing will suspend data processing, examine the groundedness of such objection, makes decision and notifies the applicant in accordance with Section 21 (2) of Infotv.

If the objection was justified, the Head of the Organisational Unit responsible for data processing will act in accordance with Section 21 (3) of Infotv.

In the event when a data subject exercises his/her rights but the case cannot be decided unambiguously, the Head of the Organisational Unit responsible for data processing may send the documents of the case together with his/her position related to the case to the internal Data Protection Officer and request his/her position, and the internal Data Protection Officer shall respond within three days.
The Company will reimburse any losses caused through unlawful processing of the data of a data subject or through breaching data security requirements, and/or will pay the restitution becoming due in the case when the data processor designated by the Company violated rights relating to personality. The Data Controller will be exempted from the liability for damages in respect of any losses and from the obligation to pay restitution if it can prove that such loss or the violation of the rights relating to personality of the data subject was caused by an inevitable cause outside the scope of data controlling. Similarly, the loss will not be reimbursed if it was a consequence of the deliberate and grossly negligent behaviour of the claimant.

The data subject may request legal remedy from or may submit his/her complaint to the Hungarian National Authority for Data Protection and Freedom of Information (1125 Budapest, Szilágyi Erzsébet fasor 22/C) or may turn to the court of justice competent in his/her place of residence or stay.

Enclosure No. 7/2

DECLARATION OF CONSENT GIVEN BY PARENTS

Data controller

name:	ELI-HU Research and Development Non-profit Limited Liability Company
short name:	ELI-HU Non-profit Llc.
corporate registration number:	Cg.06-09-015211
headquarters:	6720 Szeged, 13 Dugonics Square
e-contact:	Info@eli-alps.hu
represented by:	Lóránt Ferenc Lehrner Managing Director

Hereby I am giving my consent to ELI-HU Research and Development Non-profit Limited Liability Company (hereinafter the Data Controller) to process the personal data of my child in the interest of visiting the research centre.

purpose of data processing: enabling visits to the research centre

scope of data processed: name, date of birth and place of birth, mother's name

legal ground of data processing: consent of the data subject given in accordance with Section 5 (1) a) of Act CXII of 2011

time scope of data storage: until the achievement of the intended purpose of data processing but at most one year

data storage method: electronically and in hard copies

2. Enforcement of the rights of data subjects

A data subject may request information about the processing of his/her personal data, furthermore he/she may request the rectification of his/her personal data or its erasure – except if data processing is regulated by legal rules – such requests should be addressed to the contact possibilities of the Company.

The Company is obliged to transfer such request or objection within three days from its receipt to the Head of the Organisational Unit that is vested with responsibility and authority regarding data processing.

The Head of the Organisational Unit vested with responsibility and authority should give a properly understandable answer to the request regarding the processing of the data of the data subject, latest within 25 – in the case when right to object was exercised within 15 – days in writing from the receipt of the request/objection.

Such notification should cover the information specified in Section 15 (1) of Infotv. if the notification of the person concerned may not be refused under the said Act.

The notification in general is free of charge, the Company charges reimbursable costs only in the case specified in Section 15 (5) of Infotv.

The Data Controller refuses any application only for reasons specified in Sections 9 (1) or 19 of Infotv., which should be justified in accordance with Section 16 (2) of Infotv. in writing.

The Head of the Organisational Unit that processes data will rectify untrue data provided that the necessary data and the evidencing public deeds are available, furthermore, if causes specified in Section 17 (2) of Infotv. would prevail, he/she takes measures for the erasure of the processed personal data.

For the period necessary for the evaluation of the objection submitted by the data subject against the processing of his/her data – but at most for 5 days – the Head of the Organisational Unit responsible for data processing will suspend data processing, examine the groundedness of such objection, makes decision and notifies the applicant in accordance with Section 21 (2) of Infotv.

If the objection was justified, the Head of the Organisational Unit responsible for data processing will act in accordance with Section 21 (3) of Infotv.

In the event when a data subject exercises his/her rights but the case cannot be decided unambiguously, the Head of the Organisational Unit responsible for data processing may send the documents of the case together with his/her position related to the case to the internal Data Protection Officer and request his/her position, and the internal Data Protection Officer shall respond within three days.
The Data Controller will reimburse any losses caused through unlawful processing of the data of a data subject or through breaching data security requirements, and/or will pay the restitution becoming due in the case when the data processor designated by the Company violated rights relating to personality. The Data Controller will be exempted from the liability for damages in respect of any losses and from the obligation to pay restitution if it can prove that such loss or the violation of the rights relating to personality of the data subject was caused by an inevitable cause outside the scope of data controlling. Similarly, the loss will not be reimbursed if it was a consequence of the deliberate and grossly negligent behaviour of the claimant.

The data subject may request legal remedy from or may submit his/her complaint to the Hungarian National Authority for Data Protection and Freedom of Information (1125 Budapest, Szilágyi Erzsébet fasor 22/C) or may turn to the court of justice competent in his/her place of residence or stay.

Name and signature of the legal representative of the visitor under the age of 16

Enclosure No. 7/3

Visit to ELI-ALPS

Date of visit	
Name of the group (e.g. school, organisation, etc.)	
Name of the contact person	
Telephone number of the contact person	
E-mail address of the contact person	

	Name	**Place and date of birth**	**Mother's name**
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			
11.			
12.			
13.			
14.			
15.			
16.			
17.			
18.			
19.			
20.			
21.			
22.			
23.			
24.			
25.			
26.			
27.			
28.			
29.			
30.			
31.			
32.			
33.			
34.			
35.			

Enclosure No. 8

DATA PROTECTION INFORMATION REGARDING IMAGES RECORDED BY THE EVENT ORGANISER IN THE COURSE OF AN EVENT, PUBLICATION OF SUCH IMAGES, RECORDS

Data controller

name:	ELI-HU Research and Development Non-profit Limited Liability Company
short name:	ELI-HU Non-profit Llc.
corporate registration number:	Cg.06-09-015211
headquarters:	6720 Szeged, 13 Dugonics Square
e-contact:	Info@eli-alps.hu
represented by:	Lóránt Ferenc Lehrner Managing Director

Please be informed, that in the course of the event, the Event Organiser, **ELI-HU Research and Development Non-profit Llc.**, in its Data Controller Capacity will take video and photo images and on such images the visitors of the event could be recognisable. The Event Organiser will publish such video and photo images on electronic interfaces (Facebook, website) electronically, and in its headquarters in hard copy, and will publish them in the context of its marketing activity, however, it will not use them for advertising purposes. As regards the event, according to Section 2:48 of Act V of 2013 on the Civil Code: *"The consent of the person affected shall be required for producing or using his/her likeness or recorded voice".*

By virtue of the fact that in the knowledge of this present information you enter the premises of the event, you are giving your implied consent to the above.

purpose of data processing: strengthening the image and the brand of the Company through marketing activities, taking and using video records and photographs on this events in this context.
scope of processed data: voice and image records of data subjects and other data that can be related to the data subjects.
legal ground of data processing: consent given under Section 5 (1) a) of Infotv., and Section 2:48 (1) of Act V of 2013 on the Civil Code.
time scope of data storage: until the achievement of the intended purpose of the marketing activity

data storage method: electronically and in hard copies

You may request information about the processing of your data, also, you may request the rectification of your personal data and erasure of those data – except for data processing requested by a legal rule – by way of approaching the Company's internal Data Protection Officer. (by mail to 6728 Szeged, Budapesti út 5 or electronically at adat@eli-alps.hu).

You may request legal remedy from and submit complaint to the National Authority of Data Protection and Freedom of Information (1125 Budapest, Szilágyi Erzsébet fasor 22/C.) or to the court of justice competent in the area of your place of residence or stay

Enclosure No. 9

DECLARATION OF CONSENT FOR THE PROCESSING OF DATA CAPTURED IN THE COURSE OF VISITING AN EVENT CONDITIONAL UPON REGISTRATION

Hereby I am giving my consent that my personal data would be processed by ..... (Event Organiser) taken in the course of the event titled ..... organised by ..... (as the Event Organiser and the Controller of the registration data) in its Data Controller capacity, in accordance with the provisions stipulated in the following information material.

purpose of data processing: identification of the participant at the event

scope of processed data: name, place and date of birth, mother's name of the applicant, name of the institution represented by the applicant, position of the applicant, e-mail address, registration plate of the vehicle (if the applicant arrives by vehicle and requests parking lot), declaration from the applicant that he/she wishes to visit the visitors' centre.

legal ground of data processing: consent of the data subject in accordance with Section 5 (1) a) of Infotv.

time scope of data storage: until the finalisation of the event

data storage method: electronically

Name of the Data Processor: .....

You may request information about the processing of your data, also, you may request the rectification of your personal data and erasure of those data – except for data processing requested by a legal rule – in the manner as indicated when your data have been captured and at the contact data indicated by the data controller.

Data controller

name:	ELI-HU Research and Development Non-profit Limited Liability Company
short name:	ELI-HU Non-profit Llc.
corporate registration number:	Cg.06-09-015211
headquarters:	6720 Szeged, 13 Dugonics Square
e-contact:	Info@eli-alps.hu
represented by:	Lóránt Ferenc Lehrner Managing Director

The data subject may request legal remedy from and submit complaint to the National Authority of Data Protection and Freedom of Information (1125 Budapest, Szilágyi Erzsébet fasor 22/C) or to the court of justice competent in the area of his/her place of residence or stay.

Hereby I acknowledge the above information and am giving my consent to data processing.

Enclosure No. 10

DATA PROTECTION INFORMATION TO BE UPLOADED TO HOMEPAGE AT HTTP://WWW.ELI-HU.HU/

1. Name of Data Controller

Data controller	
name:	ELI-HU Research and Development Non-profit Limited Liability Company
short name:	ELI-HU Non-profit Llc.
corporate registration number:	Cg.06-09-015211
headquarters:	6720 Szeged, 13 Dugonics Square
e-contact:	Info@eli-alps.hu
represented by:	Lóránt Ferenc Lehrner Managing Director

2. Data Processing rules

ELI-HU Research and Development Non-profit Llc. (hereinafter the Company) on the basis of its Data Protection Regulation processes personal data in connection with this present interface. The material scope of the Regulation covers all those procedures running at any of the Company's organisational units, in the course of which personal data as specified in Section 3, point 2 of Infotv. are processed.

Personal data may exclusively be processed for a specific purpose to realize rights or fulfil obligations. The use of personal data in the control of the Company for private purposes is prohibited. Data controlling should always correspond with the purpose limitation principle.

Personal data may be processed by the Company to the minimum extent and for the shortest period necessary for the achievement of the specified and explicit purposes, where it is necessary for the implementation of certain rights and obligations. The purpose of processing must be satisfied in all stages of data processing operations, and in case the purpose of data processing has ceased or the data controlling otherwise violates the law, data should be erased.

The Company may process personal data only on the basis of the preliminary consent of the data subject – in the case of special/sensitive personal data on the basis of written preliminary consent – or on the basis of legal rule or statutory authorisation.

Prior to capturing a data, the Company in all cases informs the data subject about the purpose and the legal ground of data processing.

Employees actually processing data at the organisational units of the Company and the employees of organisations that are designated by the Company to participate in data processing or in any of the operations belonging to data processing are obliged to preserve personal data coming to their knowledge, as business secret.

If a person coming under the scope of this Regulation would gain knowledge of the fact that a personal data processed by the Company would be deficient, incomplete or outdated, he/she is obliged to rectify same or arrange for its rectification by the employee responsible for data capturing.

Data protection obligations applicable to natural or legal persons or organisations without legal personality that are designated by the Company to perform data processing activities should be enforced in the service contract concluded with the data processor.

The ruling Senior Executive Officer of the Company will in due consideration of the specific features of the Company determine the data protection organisation and the scopes of responsibilities and authorities related to such activity, and designate a person who is responsible for supervising data processing.

In the course of their work, the members of the staff of the Company ensure that unauthorised persons would not view personal data and that personal data should be stored and located in such manner that they would not be accessible, readable, changeable and/or destroyable by unauthorised persons.

The data protection system of the Company should be supervised by the Senior Executive Officer through a data protection officer appointed or designated by him/her.

The homepage operated by the Company can be accessed by anyone without revealing his/her identity and giving his/her personal data, also, information can be retrieved from the homepage and the linked sites freely and without restrictions. Meanwhile the homepage gathers non-personal information about its visitors without any restriction. From these pieces of information personal data cannot be retrieved, therefore this is not constituted as data controlling coming under the scope of Infotv.

On its homepage the Company utilises a web analytics service named Google Analytics. Google Analytics applies cookies and text files downloaded on the computer of the visitor of the website, the aim of which is the facilitation of the analysis of the use of the website. Pieces of information generated by the cookies and related to the use of the website (IP-address of the visitor of the website) are transferred to the server of Google located in the United States of America and are stored there. Google does not interconnect information generated by the cookies with other data, therefore, according to the data protection regulation in force it cannot be deemed to be data processing. By way of appropriately setting his/her browser, the visitor of the website can refuse the application of cookies. By virtue of using the website, the visitor of the homepage consents the processing of his/her data in the manner and/or the purpose as discussed above.

Pieces of information so acquired are used by Google for the evaluation of the use of the homepage by data subjects, for analyses, compilation of reports on operations performed on the website, and for delivering other services related to operations performed on the homepage and to internet usage.

If any operation on the homepage requires logging in, the Company handles personal data of the visitors in the following manner:

purpose of data processing: identification of the visitors of the homepage; making electronic services available for them
scope of processed data: starting and finishing time of the visit of the user, and/or in certain cases – dependently upon the settings of the user's computer – the type of the browser and the operating system, IP address, other captured data (cookies) in the case of operation requiring logging in: name, e-mail address.
legal ground of data processing: consent of the data subject in accordance with Section 5 (1) a) of Infotv.
time scope of data storage: until the achievement of the purpose of data processing, for maximum 2 years
data storage method: electronically

3. Enforcement of the rights of data subjects

A data subject may request information about the processing of his/her personal data, furthermore he/she may request the rectification of his/her personal data or its erasure – except if data processing is regulated by legal rules – such requests should be addressed to the contact possibilities of the Company.

The Company is obliged to transfer such request or objection within three days from its receipt to the Head of the Organisational Unit that is vested with responsibility and authority regarding data processing.

The Head of the Organisational Unit vested with responsibility and authority should give a properly understandable answer to the request regarding the processing of the data of the data subject, latest within 25 – in the case when right to object was exercised within 15 – days in writing from the receipt of the request/objection.

Such notification should cover the information specified in Section 15 (1) of Infotv. if the notification of the person concerned may not be refused under the said Act.

The notification in general is free of charge, the Company charges reimbursable costs only in the case specified in Section 15 (5) of Infotv.

The Company refuses any application only for reasons specified in Sections 9 (1) or 19 of Infotv., which should be justified in accordance with Section 16 (2) of Infotv. in writing.

The Head of the Organisational Unit that processes data will rectify untrue data provided that the necessary data and the evidencing public deeds are available, furthermore, if causes specified in Section 17 (2) of Infotv. would prevail, he/she takes measures for the erasure of the processed personal data.

For the period necessary for the evaluation of the objection submitted by the data subject against the processing of his/her data – but at most for 5 days – the Head of the Organisational Unit responsible for data processing will suspend data processing, examine the groundedness of such objection, makes decision and notifies the applicant in accordance with Section 21 (2) of Infotv.

If the objection was justified, the Head of the Organisational Unit responsible for data processing will act in accordance with Section 21 (3) of Infotv.

In the event when a data subject exercises his/her rights but the case cannot be decided unambiguously, the Head of the Organisational Unit responsible for data processing may send the documents of the case together with his/her position related to the case to the internal Data Protection Officer and request his/her position, and the internal Data Protection Officer shall respond within three days.

The Company will reimburse any losses caused through unlawful processing of the data of a data subject or through breaching data security requirements, and/or will pay the restitution becoming due in the case when the data processor designated by the Company violated rights relating to personality. The Data Controller will be exempted from the liability for damages in respect of any losses and from the obligation to pay restitution if it can prove that such loss or the violation of the rights relating to personality of the data subject was caused by an inevitable cause outside the scope of data controlling. Similarly, the loss will not be reimbursed if it was a consequence of the deliberate and grossly negligent behaviour of the claimant.

The data subject may request legal remedy from or may submit his/her complaint to the Hungarian National Authority for Data Protection and Freedom of Information (1125 Budapest, Szilágyi Erzsébet fasor 22/C) or may turn to the court of justice competent in his/her place of residence or stay.

Enclosure No. 11

INFORMATION ABOUT NEWSLETTER DISTRIBUTION

Name of Data Controller

Data Controller	
name:	ELI-HU Research and Development Non-profit Limited Liability Company
short name:	ELI-HU Non-profit Kft.
corporate registration number:	Cg.06-09-015211
headquarters:	6720 Szeged, 13 Dugonics Square.
e-contact	Info@eli-alps.hu
represented by:	Lóránt Ferenc Lehrner Managing Director

Please be informed that you have the possibility to subscribe to our newsletter distribution service and therefore you may get information about the products, services, actions of ELI-HU Research and Development Non-profit Llc. and about other interesting news. Newsletter will be sent for ..... occasions; we will process no other data of you but your e-mail address and your name. In any phase of the data processing you have the possibility to unsubscribe from our newsletter by sending your message to the following e-mail address: .....

purpose of data processing: sending newsletter for subscribers

scope of processed data: username, e-mail address

legal ground of data processing: consent of the data subject in accordance with Section 5 (1) a) of Infotv.

time scope of data storage: until the data subject unsubscribes

data storage method: electronically

Enforcement of the rights of data subjects

A data subject may request information about the processing of his/her personal data, furthermore he/she may request the rectification of his/her personal data or its erasure – except if data processing is regulated by legal rules – such requests should be addressed to the contact possibilities of the Company.

The Company is obliged to transfer such request or objection within three days from its receipt to the Head of the Organisational Unit that is vested with responsibility and authority regarding data processing.

The Head of the Organisational Unit vested with responsibility and authority should give a properly understandable answer to the request regarding the processing of the data of the data subject, latest within 25 – in the case when right to object was exercised within 15 – days in writing from the receipt of the request/objection.

Such notification should cover the information specified in Section 15 (1) of Infotv. if the notification of the person concerned may not be refused under the said Act.

The notification in general is free of charge, the Company charges reimbursable costs only in the case specified in Section 15 (5) of Infotv.

The Company refuses any application only for reasons specified in Sections 9 (1) or 19 of Infotv., which should be justified in accordance with Section 16 (2) of Infotv. in writing.

The Head of the Organisational Unit that processes data will rectify untrue data provided that the necessary data and the evidencing public deeds are available, furthermore, if causes specified in Section 17 (2) of Infotv. would prevail, he/she takes measures for the erasure of the processed personal data.

For the period necessary for the evaluation of the objection submitted by the data subject against the processing of his/her data – but at most for 5 days – the Head of the Organisational Unit responsible for data processing will suspend data processing, examine the groundedness of such objection, makes decision and notifies the applicant in accordance with Section 21 (2) of Infotv.

If the objection was justified, the Head of the Organisational Unit responsible for data processing will act in accordance with Section 21 (3) of Infotv.

In the event when a data subject exercises his/her rights but the case cannot be decided unambiguously, the Head of the Organisational Unit responsible for data processing may send the documents of the case together with his/her position related to the case to the internal Data Protection Officer and request his/her position, and the internal Data Protection Officer shall respond within three days.
The Company will reimburse any losses caused through unlawful processing of the data of a data subject or through breaching data security requirements, and/or will pay the restitution becoming due in the case when the data processor designated by the Company violated rights relating to personality. The Data Controller will be exempted from the liability for damages in respect of any losses and from the obligation to pay restitution if it can prove that such loss or the violation of the rights relating to personality of the data subject was caused by an inevitable cause outside the scope of data controlling. Similarly, the loss will not be reimbursed if it was a consequence of the deliberate and grossly negligent behaviour of the claimant.

The data subject may request legal remedy from or may submit his/her complaint to the Hungarian National Authority for Data Protection and Freedom of Information (1125 Budapest, Szilágyi Erzsébet fasor 22/C) or may turn to the court of justice competent in his/her place of residence or stay.

Enclosure No. 12

INFORMATION ABOUT DATA PROCESSING IN CONNECTION WITH BRAND BUILDING

Name of Data Controller

Data Controller

name:	ELI-HU Research and Development Non-profit Limited Liability Company
short name:	ELI-HU Non-profit Kft.
corporate registration number:	Cg.06-09-015211
headquarters:	6720 Szeged, 13 Dugonics Square.
e-contact	Info@eli-alps.hu
represented by:	Lóránt Ferenc Lehrner Managing Director

Please be informed that in the course of your participation in the sweepstakes organised by our Company, your name and contact data will be captured

purpose of data processing: organisation and arrangement of sweepstakes

legal ground of data processing: consent of the data subject in accordance with Section 5 (1) a) of Act CXII of 2011

scope of processed data: name, telephone number and e-mail address

time scope of data controlling: until the notification of the winner

data storage method: hard copies and electronically

3. Enforcement of the rights of data subjects

A data subject may request information about the processing of his/her personal data, furthermore he/she may request the rectification of his/her personal data or its erasure – except if data processing is regulated by legal rules – such requests should be addressed to the contact possibilities of the Company.

The Company is obliged to transfer such request or objection within three days from its receipt to the Head of the Organisational Unit that is vested with responsibility and authority regarding data processing.

The Head of the Organisational Unit vested with responsibility and authority should give a properly understandable answer to the request regarding the processing of the data of the data subject, latest within 25 – in the case when right to object was exercised within 15 – days in writing from the receipt of the request/objection.

Such notification should cover the information specified in Section 15 (1) of Infotv. if the notification of the person concerned may not be refused under the said Act.

The notification in general is free of charge, the Company charges reimbursable costs only in the case specified in Section 15 (5) of Infotv.

The Company refuses any application only for reasons specified in Sections 9 (1) or 19 of Infotv., which should be justified in accordance with Section 16 (2) of Infotv. in writing.

The Head of the Organisational Unit that processes data will rectify untrue data provided that the necessary data and the evidencing public deeds are available, furthermore, if causes specified in Section 17 (2) of Infotv. would prevail, he/she takes measures for the erasure of the processed personal data.

For the period necessary for the evaluation of the objection submitted by the data subject against the processing of his/her data – but at most for 5 days – the Head of the Organisational Unit responsible for data processing will suspend data processing, examine the groundedness of such objection, makes decision and notifies the applicant in accordance with Section 21 (2) of Infotv.

If the objection was justified, the Head of the Organisational Unit responsible for data processing will act in accordance with Section 21 (3) of Infotv.

In the event when a data subject exercises his/her rights but the case cannot be decided unambiguously, the Head of the Organisational Unit responsible for data processing may send the documents of the case together with his/her position related to the case to the internal Data Protection Officer and request his/her position, and the internal Data Protection Officer shall respond within three days.
The Company will reimburse any losses caused through unlawful processing of the data of a data subject or through breaching data security requirements, and/or will pay the restitution becoming due in the case when the data processor designated by the Company violated rights relating to personality. The Data Controller will be exempted from the liability for damages in respect of any losses and from the obligation to pay restitution if it can prove that such loss or the violation of the rights relating to personality of the data subject was caused by an inevitable cause outside the scope of data controlling. Similarly, the loss will not be reimbursed if it was a consequence of the deliberate and grossly negligent behaviour of the claimant.

The data subject may request legal remedy from or may submit his/her complaint to the Hungarian National Authority for Data Protection and Freedom of Information (1125 Budapest, Szilágyi Erzsébet fasor 22/C) or may turn to the court of justice competent in his/her place of residence or stay.

Enclosure No. 13/1

AREA WATCHED BY CAMERAS

Sector I

(information board to be posted at the point of entrance to the watched premises)

Please be informed that **ELI-HU Research and Development Non-profit Llc. (hereinafter the Company)** in accordance with the provisions stipulated in Act CXXXIII of 2005 on Security Services and the Activities of Private Investigators (hereinafter Szvtv.), in the territory of the facility operates electronic surveillance system. The electronic security technical systems capture and store personal data and images in accordance with the provisions stipulated in the legal rules in force.

Registration number of processing personal data recorded and captured: NAIH-

Aim of capturing and storing personal data:
safe storage, handling and transportation of properties, equipments and money, that under the Act on the Criminal Code qualifies as at least of significant value
Legal ground of capturing and storing personal data and images:
- implied consent of the data subject [Section 30 (2) of Szvtv.]

Data captured by the surveillance system may be accessed by:
- the Senior Executive Officer of the Company or a person designated by him/her
- a court of justice or other competent authority in the interest of usage in court or other authoritative proceedings.

Place of storage of personal data and images: (insert here the address where the Company stores the records!)

Time scope of storage of personal data and images:
if the record is not utilised, it will be erased within 30, say thirty days passing from recording [Section 31 (3) c) of Szvtv.]
if following the certification of rights of lawful interests, the Company was requested not to destroy the record, meanwhile, request was not submitted, then the record will be erased within 30, say thirty days from such request [Section 31 (6) of Szvtv.]

If the personal data and images captured and stored would not be utilised within the above periods, the Company will destroy them or erase from its system. Utilisation shall mean that an image or personal data captured would be used in a court or other authoritative proceeding as evidence.

The person whose right or legal interest would be interfered by the capturing of his/her image or other personal data, may within the above deadline – following the certification of his/her legal interest – request the Company not to destroy or not to erase such data. In response to the request of a court of justice or other authority, the captured image or other personal data should immediately be sent to the court of justice or authority. If within thirty days from the day when such disregarding of destruction was requested, request from the court or other authority would not be received, such captured image or personal data will be destroyed or erased by the Company, except if the period of data storage has not been expired.

The person who is concerned by such recorded and stored personal data or image may submit a written query to the Senior Executive Officer of the Company or to the internal Data Protection Officer (mailing address: 6720 Szeged, Dugonics tér 13, e-mail: adat@eli-alps.hu) where in accordance with the provisions stipulated in Act CXII of 2011 on the Right of Information Self-Determination and Freedom of Information he/she may request information about the processing of his/her data, rectification and/or erasure of his/her personal data, protest against the processing of his/her personal data and in the case of violation of his/her rights turn to the court of justice and request damages.

Enclosure No. 13/2

AREA WATCHED BY CAMERAS

Sector II
(information board to be posted at the point of entrance to the watched premises)

Please be informed that **ELI-HU Research and Development Non-profit Llc. (hereinafter the Company)** in accordance with the provisions stipulated in Act CXXXIII of 2005 on Security Services and the Activities of Private Investigators (hereinafter Szvtv.), in the territory of the facility operates electronic surveillance system. The electronic security technical systems capture and store personal data and images in accordance with the provisions stipulated in the legal rules in force.

Registration number of processing personal data recorded and captured: NAIH-

Aim of capturing and storing personal data:
storage of hazardous materials
Legal ground of capturing and storing personal data and images:
- implied consent of the data subject [Section 30 (2) of Szvtv.]

Data captured by the surveillance system may be accessed by:
- the Senior Executive Officer of the Company or a person designated by him/her
- a court of justice or other competent authority in the interest of usage in court or other authoritative proceedings.

Place of storage of personal data and images: (insert here the address where the Company stores the records!)

Time scope of storage of personal data and images:
if the record is not utilised, it will be erased within 30, say thirty days passing from recording [Section 31 (3) d) of Szvtv.]
if following the certification of rights of lawful interests, the Company was requested not to destroy the record, meanwhile, request was not submitted, then the record will be erased within 30, say thirty days from such request [Section 31 (6) of Szvtv.]

If the personal data and images captured and stored would not be utilised within the above periods, the Company will destroy them or erase from its system. Utilisation shall mean that an image or personal data captured would be used in a court or other authoritative proceeding as evidence.

The person whose right or legal interest would be interfered by the capturing of his/her image or other personal data, may within the above deadline – following the certification of his/her legal interest – request the Company not to destroy or not to erase such data. In response to the request of a court of justice or other authority, the captured image or other personal data should immediately be sent to the court of justice or authority. If within thirty days from the day when such disregarding of destruction was requested, request from the court or other authority would not be received, such captured image or personal data will be destroyed or erased by the Company, except if the period of data storage has not been expired.

The person who is concerned by such recorded and stored personal data or image may submit a written query to the Senior Executive Officer of the Company or to the internal Data Protection Officer (mailing address: 6720 Szeged, 13 Dugonics Square, e-mail: adat@eli-alps.hu) where in accordance with the provisions stipulated in Act CXII of 2011 on the Right of Information Self-Determination and Freedom of Information he/she may request information about the processing of his/her data, rectification and/or erasure of his/her personal data, protest against the processing of his/her personal data and in the case of violation of his/her rights turn to the court of justice and request damages.

Enclosure No. 14/1

REGISTRY OF PERSONS VESTED WITH PERMANENT RIGHT TO VIEW IMAGES

Name of person vested with access right	Position	Date of granting access rights	Date of withdrawal of access rights
Ferenc Lóránt Lehrner	Managing Director	12.05.2017	
Attila Hódi	Security Officer	12.05.2017	
dr. Viktória Papp	Internal Data Protection Officer	12.05.2017	

Enclosure No. 14/2

PROTOCOL TAKEN ON THE VIEWING OF IMAGES RECORDED WITH CAMERAS

PROTOCOL

1. Data of the record viewed:

   1.1 Record location (location where the camera is operated):

   1.2 Time scope/duration of the record viewed (expressed in date, hour, minute format) or the time of starting and terminating the viewing of a real time image:

2. Persons participating in viewing data (ground of eligibility for viewing records):

3. Location and time of viewing data:

4. Reason and purpose of viewing data:

5. Proposal regarding further data processing based on viewing data (please underline as appropriate):
   - record should be used for starting or continuing further (civil/criminal) proceeding,
   - handover of the relevant record to an authority on the basis of the request of the competent authority,
   - destruction of the record in accordance with the legal rules, termination of data processing,
   - other: .....

6. Other relevant events perceived in the course of data viewing, related to the circumstances:

Date: .....

.....
signature
[name of the person vested with data viewing]

.....
signature

Enclosure No. 15/1

PROTOCOL TAKEN ON THE BLOCKING OF IMAGES RECORDED WITH CAMERAS

PROTOCOL

INITIATION OF BLOCKING

Blocking initiated by:

Description of the reasons for initiation of blocking:

Data of the records proposed for blocking:

- record location (location where the camera is operated):
- time scope/duration of the record proposed for blocking (expressed in date, hour, minute format):

Purpose of blocking (please underline as appropriate)

- record should be used for starting or continuing further (civil/criminal) proceeding,
- handover of the relevant record to an authority on the basis of the request of the competent authority,
- destruction of the record in accordance with the legal rules, termination of data processing,
- other:

Date: .....

.....
signature of the initiator

DECISION ON BLOCKING

Person making decision on blocking

□ person designated to supervise data processing through camera system
□ internal Data Protection Officer

Decision

□ request for blocking agreed; blocking is executed
□ request for blocking is ungrounded; blocking will not be executed
□ decision on blocking cannot be passed on the basis of the available data; request for blocking is returned to the initiator of blocking, for the clarification of further data of relevance

Date: .....

.....
signature of the person deciding on blocking

BLOCKING

Location and time of blocking:

Person responsible for blocking:

The blocked record:

□ has been handed over to the competent acting authority,

□ has been handed over to the person responsible for supervising data processing through camera system, in accordance with the data protection regulation regarding Electronic surveillance system.

Date: .....

.....
signature of the person responsible for blocking

RELEASE OF A RECORD FROM BLOCKING

Blocking of the record has been released:

□ the period available for storing the blocked record has passed in vain and the blocked record has been erased,

□ the period available for storing the blocked record has passed in vain but the blocked record has not been erased because the data processing period according to the general rule has not yet passed.

Date: .....

.....
signature of the person deciding on blocking

Enclosure No. 15/2

REGISTRY OF PERSONS VESTED WITH BLOCKING ELIGIBILITY

Name of person vested with blocking eligibility	Position	Date of granting access rights	Date of withdrawal of access rights
dr. Viktória Papp	Legal Counsel	12.05.2017	

Enclosure No. 16

DATA PROTECTION INFORMATION MATERIAL FOR PERSONS ENTERING THE COMPANY'S PREMISES

Security tasks in the facility are performed under service contract:

XxX Limited liability company

- Seat: XxX
- Corporate registration number: XxX
- Represented by: XxX

Principal and also Data Controller

name:	ELI-HU Research and Development Non-profit Limited Liability Company (hereinafter the Company)
short name:	ELI-HU Non-profit Kft.
corporate registration number:	Cg.06-09-015211
headquarters:	6720 Szeged, 13 Dugonics Square.
e-contact	Info@eli-alps.hu
represented by:	Lóránt Ferenc Lehrner Managing Director

Hereby we inform our visitors that the facility in Szeged (6728 Szeged, 5 Budapesti Street) is separated to several zones from the security and access eligibility aspects.

The green zone is the area that is open for clients; this area may be accessed by anyone without authentication of identity or any check. (except for events)

The yellow zone is the area of the visitors' centre where visitors may enter following preliminary registration. After the authentication of the identity, the visitor will be provided with a badge. Registration will be executed in accordance with the provisions stipulated in the chapter about the visitors' centre.

Into the area of the orange zone exclusively employees and persons employed under other form of employment relationship may enter.

The red zone is intensely protected, it may be accessed by a narrow scope of employees (e.g. server room, security surveillance, etc.).

The black zone is the so-called laser space. This area may be accessed only by persons vested with distinguished access rights.

The white zone is a separated area where the kitchen can be found which is operated by an external firm.

Visitors are reminded that on the ground of the statutory authorisation granted in Section 26 (1) of Act CXXXIII of 2005 on Security Services and the Activities of Private Investigators (hereinafter Szvtv.), the Security Guards of XxX Llc. in the course of safeguarding the facilities of the Principal, which do not qualify as public areas are entitled for the following:

a) request persons entering to or staying in the premises to authenticate their identity, reveal the aim of entering or staying, and in response to the refusal of the above or in the case of the obvious falsehood of the data so revealed, prohibit the entry or the stay of the person concerned and request him/her to leave;

b) request the person entering or leaving the premises to present documents related to baggage and/or to present bill of lading, bill of transportation;

c) request the person staying in or leaving the premises to enable the surveillance of his/her packages, vehicle, as well as the cargo, always within the statutory frameworks;

d) request law violating persons to terminate such conduct;

e) apply electronic security system;

f) apply instruments for detecting weapons and explosive materials, in the course of checking persons entering the premises, and prohibit bringing into the premises any means that are extremely dangerous for public safety.

Visitors are reminded that it is prohibited to bring into the premises of the facility any means/devices listed in the enclosure of Government Decree 175/2003 (X. 28.) Korm. on means that are extremely dangerous for public safety:

a) thrusting or cutting device whose thrusting length or cutting edge exceeds 8 cm, furthermore, irrespective of the size of the thrusting length or the cutting edge throwing star, spring assisted knife or any device suitable for shooting, thrusting or cutting, or any tool or other object apt for causing bodily injury (specifically bow, cross bow, French knife, harpoon gun, catapult, slingshot);

b) any tool typically usable for knocking which increases the strength and the impact of knocking (specifically: slapjack, boxer);

c) clubs or weights connected with chain or other flexible material;

d) any device that can spray substances that through the irritation of the eye or the mucous membrane or the skin makes a person incapable to attack (gas spray);

e) any device that because of the nature of imitation and the scale of its design is similar to a firearm to such extent that is apt for counterfeiting (replica firearm);

f) any device that uses electric discharge to incapacitate a person (electric shocker).

g) any mean that serves for illegally opening or breaking locks (specifically: picklock, mechanic or electronic lock opening devices).

Visitors are reminded that in the interest of performing its tasks, XxX Llc. on the ground of the statutory authorisation granted in Sections 30 (1) and 32 (1) of Szvtv. may in the premises of the facility use electronic surveillance system and electronic access control system. Electronic safety technique systems capture and store personal data and images in accordance with the provisions stipulated in the legal rules in force.

In the course of the application of the electronic access control system, the period of the storage of personal data is in correspondence with the storage periods in accordance with Szvtv.

purpose of data processing: security check in the course of entrances and departures
scope of processed data: name, time of entrance and departure, identification number of the entering person
legal ground of data processing: the consent of the data subject in accordance with Section 5 (1) a) of Infotv. and Section 32 of Act CXXXIII of 2005.
time scope of data storage:

- in the case of eligibility for regular entrances, the authentication data (name and identification number) necessary for the operation of the system will be deleted by the Company immediately after the termination of such eligibility,

- in the case of eligibility for regular entrances, those data that were generated in the course of the operation of the system will be deleted by the Company concurrently with the termination of such eligibility but latest after 6 months from the generation of such data.

data storage method: electronically

In the case of suppliers, in accordance with the AEO (Authorised Economic Operator) standard, the data of the entering persons should preliminarily be submitted to the gatekeepers: name of the driver, mother's name (in certain cases father's name), date of birth, place of birth, vehicle registration number and the data of the cargo.

Data in such cases are captured in hard copy by the gatekeeper service.

purpose of data processing: security surveillance in the course when suppliers access the premises

scope of processed data: name of the driver, mother's name (in certain cases father's name), date of birth, place of birth, vehicle registration number and the data of the cargo.

legal ground of data processing: the consent of the data subject in accordance with Section 5 (1) a) of Infotv. and Section 32 of Act CXXXIII of 2005.

time scope of data storage:

identification data handled for access controlling purposes should be destroyed

- in the case of eligibility for regular entrances immediately after the termination of such eligibility,
- in the case of occasional entries after 24 hours passing from departure

data storage method: in hard copy

Management of extraordinary security events

Extraordinary event shall mean an event or circumstance that deviates from the average, which therefore may lead to severe consequences regarding life, corporeal integrity of persons staying in the facility or regarding properties to be found there, or there are realistic chances for leading to such consequences and therefore severe disturbance in the operation of the facility could be caused.

The Security Guards employed by the contracted service provider will take protocol on any event within the premises that is of relevance from the security aspect. Such protocol should contain the following data: date of taking protocol, name of the member of the staff of the security service, his/her signature, name of the person investigated, his/her signature, name at birth, place, date of birth, mother's name, residential address, place of stay of the person investigated and the description of the event. These data are relative personal data, therefore – under Infotv. – they might become personal data.

purpose of data processing: investigation of extraordinary security event

scope of processed data: date of capturing the protocol, name of the member of the staff of the security service, his/her signature, name of the person investigated, his/her signature, name at birth, place and time of birth, mother's name, residential address, place of stay of the person investigated and the description of the event

legal ground of data processing: consent of the data subject in accordance with Section 5 (1) a) of Infotv.

time scope of data storage: investigation of the event, the deadline available for enforcing claims regarding rights and obligations stemming therefrom.

data storage method: in hard copy

Security surveillances

In the interest of protecting properties, on the basis of the authorisation ensured by Section 26 of Szvtv., the Company conducts package, cabinet/locker, vehicle and cargo surveillance.

Such surveillance may be conducted by the Security Guard for the purpose of enforcing his/her obligations stemming from the contract, following notification as regards the reason and the aim of the measure, in those cases when

- it can be suspected with good ground that the person concerned keeps a thing acquired by criminal action or misdemeanour, and the safeguarding of such property is the contractual obligation of the Security Guard,
- such thing is not handed over despite the relevant request, and
- such measure is necessary for preventing or halting a law violating act.

If the surveillance is closed with tangible result, the Security Guard takes a protocol on the surveillance of the extraordinary event, and such protocol will be subjected to the relevant rules of data processing.

***

Please be informed that the Company applies closed circuit camera surveillance system in its site under 5 Budapesti Street, Szeged 6728.

The cameras form the Company's own property and are operated by the Company.

The camera records are stored on the local servers.

In the case of terror hazard the Constitution Protection Office may have access to the records in view of the fact that the site is a distinguished national security facility.

The storage and use of images created by the electronic surveillance system are governed by the following rules in due consideration of the provisions stipulated in Szvtv.:

Sectors of the electronic surveillance system

The Company distinguishes the areas watched by the electronic surveillance system into two separate categories according to the aim of surveillance.
The first category is so-called Sector I where the legal rule that governs the applied electronic surveillance system is Section 31 (3) c) of Szvtv., because the aim of surveillance is the safe storage, handling and transportation of properties and equipments, money, securities, noble metal, precious stones that are of at least significant value as described in the Act on the Criminal Code.

The second category is the so-called Sector II where the legal rules that governs the applied electronic surveillance system is Section 31 (3) d) of Szvtv., because the aim of the surveillance is the safeguarding of hazardous materials.

Method of and deadline set for erasure of records generated by the electronic surveillance system

Sector I
As per Section 31 (3) c) of Szvtv. at the units specified by the Company, in the interest of the safe storage, handling and transportation of properties and equipments, money that are of at least significant value as described in the Act on the Criminal Code, records are stored for 30 days.

Sector II
As per Section 31 (3) d) of Szvtv., records taken in the interest of safeguarding hazardous materials are kept by the Company for 30 days.

In both cases the Company from among the rights that the data subjects are vested with guarantees those specified in Szvtv., i.e. if a record interferes with a person's rights or lawful interests, such person may within the deadline set for erasure as specified above (thirty days) request the data controller not to destroy and/or not to erase such record provided that he/she can certify his/her right or legal interest. The decision about such request will be passed by the internal Data Protection Officer of the Company within the shortest possible deadline. The record so distinguished should be saved and handed over to the internal Data Protection Officer who will arrange for its safeguarding in accordance with the data protection rules corresponding with this present Regulation. In response to any request from a court or other authority, the record should be sent to the court or authority without delay. If such request would not be received within thirty days from the day when the request for disregarding destruction was received, such record will be erased.

Warranty rules related to electronic surveillance

Through the electronic surveillance system, the Company interferes with the privacy of the data subject only to the necessary extent.

The Company does not apply electronic surveillance for whatever reason and in whatever manner in the following cases:

- surveillance of the work intensity of the employee,
- influencing the behaviour conducted by employees at the work premises,
- in sensitive areas, specifically changing room, shower, toilette,
- in areas where employees spend their relax time or breaks, specifically relaxation rooms, smoking areas,
- public areas.

However, the Company may apply electronic surveillance in order to gain confidence that the employees observe the regulations related to them in the interest of health safe and secure work practices.

Viewing images recorded by the cameras

In order that the Company would interfere with the privacy of the data subjects to the least extent, the images recorded by the electronic surveillance system may be accessed by designated persons only.

Within the organisational system of the Company, only the person designated in this present Regulation may view recorded images.

Protocol should be taken on the viewing of camera images.

Blocking of camera images

Blocking of images taken by the cameras may be required only by a person designated to supervise data processing through the Company's camera system or the internal Data Protection Officer if he/she has been appointed.

Blocking of camera images may be initiated by:

- a person vested by the Company with right to view if in the course of viewing such images he/she would perceive any circumstance that would endanger the aim to be achieved by the electronic surveillance system,
- anybody, whose rights or lawful interests are interfered by the records.

Blocking of the camera records can be requested with an application addressed to the person designated to supervise data processing through the camera system and concurrently to the internal data protection officer if such person has been designated.

The decision about blocking will be passed by the person designated by the company for supervising data processing through the camera system within the shortest possible time (in agreement with the internal Data Protection Officer if such person has been designated).

The Company takes a protocol on blocking images recorded by the cameras, in which the time of viewing and blocking, its purpose furthermore the event giving reason for blocking and the indication of further use should be stated.

Persons vested with blocking eligibility

The Company keeps a registry on the scope of persons entitled to block images. Such registry contains the name and position of the person vested with blocking rights, date of issuing such blocking right, date of withdrawal of blocking right. The Company keeps such data for 5 years counted from withdrawal. The registry of persons vested with blocking rights is contained Enclosure No. of the regulation.

Sector I
purpose of data processing: storage, handling and transportation of properties, equipments and money qualifying as at least of significant value according to the Act on the Criminal Code
scope of processed data: portrait of the data subject, data that can be acquired with the camera image (place of stay, duration of stay),
legal ground of data processing: implied consent of the data subject [Section 30 (2) of Szvtv.]
time scope of data storage:

- if the record is not utilised, it will be erased within 30, say thirty days passing from recording [Section 31 (3) c) of Szvtv.]
- if following the certification of rights of lawful interests, the Company was requested not to destroy the record, meanwhile, request was not submitted, then the record will be erased within 30, say thirty days from such request [Section 31 (6) of Szvtv.]

method of data processing: electronically

Sector II
purpose of data processing: safeguarding hazardous materials
scope of processed data: portrait of the data subject, data that can be acquired with the camera image (place of stay, duration of stay),
legal ground of data processing: implied consent of the data subject [Section 30 (2) of Szvtv.]

- if the record is not utilised, it will be erased within 30, say thirty days from recording [Section 31 (3) d) of Szvtv.]
- if following the certification of rights of lawful interests, the Company was requested not to destroy the record, meanwhile, request was not submitted, then the record will be erased within 30, say thirty days passing from such request [Section 31 (6) of Szvtv.]

method of data processing: electronically

You may request information about the processing of your data, also, you may request the rectification of your personal data and erasure of those data – except for data processing requested by a legal rule – in the manner as indicated when your data have been captured and at the contact data indicated by the data controller.

The data subject may request legal remedy from or may submit his/her complaint to the Hungarian National Authority for Data Protection and Freedom of Information (1125 Budapest, Szilágyi Erzsébet fasor 22/C) or may turn to the court of justice competent in his/her place of residence or stay.

Enclosure No. 17

DATA PROTECTION – DATA PROCESSING ARTICLE TO BE INCLUDED IN CONTRACTS

Data protection article to be included in employment contract:

In the course of his/her employment relationship, certain information, specifically business plans, trade secrets, customer data and other proprietary information, as well as personal data coming under the scope of the Infotv. (together: information) revealed or to be revealed in the future for the employee may be stored by the employee exclusively on the electronic devices forming the property of the Company, all other storage is prohibited. In all such cases where the employee processes information not in correspondence with the provisions stipulated in the Company's Data Protection Regulation, he/she under the Infotv. will become data controller and in the course of exercising rights and satisfying obligations related to data controlling will replace the Company and at the same time establishes legal ground for the termination of his/her employment relationship with immediate effect in accordance with Section 78 (1) a) of Act I of 2012 on Labour Code (hereinafter: Mt.) *("An employer or employee may terminate an employment relationship without notice if the other party wilfully or by gross negligence commits a grave violation of any substantive obligations arising from the employment relationship.")*

Data protection article to be included in other employment legal relationship (service contract, etc.):

In the course of the legal relationship established between the Company and the person performing the work, the Company obliges the co-worker to handle certain information revealed or to be revealed in the future, specifically business plans, trade secrets, customer's data and other proprietary information as well as personal data coming under the scope of the Infotv. (together: information) on the ground of the Company's Data Protection Regulation. If the worker processes information not in accordance with the provisions stipulated in the Company's Data Protection Regulation, then according to the Infotv. he/she will become data controller and in the course of exercising rights and satisfying obligations related to data controlling will replace the Company as data controller and at the same time the Company will become entitled to cancel its legal relationship established with the co-worker with immediate effect.

Enclosure No. 18

DATA PROTECTION SUPPLEMENTARY NOTE TO BE INSERTED IN THE DATA CAPTURING PRINTED FORMS

ELI-HU Research and Development Non-profit Llc. informs you that personal data to be captured in the course of completion of this present printed form will be processed in accordance with the provisions stipulated in Act CXII of 2011 on the Right of Informational Self-Determination and Freedom of Information and the Company's Data Protection Regulation.

Enclosure No. 19

PERMISSION FOR TAKING THE SERVER ROOM KEY

Permanent permission:

KEY POSSESSION PERMISSION

The owner of this present permission
NAME:
position:
is entitled to keep the key of the server room until the withdrawal of this present permission.

Name of the issuer of this permission:

Date,

Signature

Occasional permission:

PERMISSION TO TAKE KEY

The owner this present permission
NAME:
position:
is entitled to take the key of the server room from ..... (date, time) and keep it until ..... (date, time).

Name of the issuer of the permission:

Date,

Signature

Enclosure No. 20

REGISTER OF PERSONS ENTITLED TO TAKE THE KEY OF THE SERVER ROOM

Name of the person entitled to take the key	Position	Date of issuing permission	Date of withdrawal of permission	Type of entitlement (permanent/ occasional)

Enclosure No. 21

DATA DESTRUCTION PROTOCOL

...../20...

DATA DESTRUCTION PROTOCOL

To be completed by the employee responsible for data erasure!

Employee responsible for data destruction

name:
mother's name:
place and date of birth:
identification number:

Destruction permitted by:

Members of the three-strong committee present at the data destruction:

1.
2.
3.

Place and time (date-hour-minute) of data destruction:

Subject matter destroyed:[3]

Data destruction method

❑ shredding machine
❑ burning
❑ smashing
❑ grinding
❑ other:

.....
signature of the employee responsible for data destruction

Signatures of the members of the three-strong committee:

....
1. 2. 3.

[3] e.g.: invoices, invoice books not in use from 1 January 2008; resumes, etc. received in year 2014

Enclosure No. 22/1

DATA PROTECTION / PRIVACY INCIDENT REGISTER

On the basis of Section 15 (1) a) of Act CXII of 2011 on the Right of Informational Self-Determination and Freedom of Information, in order to check measures related to privacy incidents, and for informing data subjects on privacy incidents, the Company keeps a register on privacy incidents.

The Company files all privacy incidents, and compiles register from the incident recording sheets so filed.

...../20.../AVINC[4]

PRIVACY INCIDENT RECORDING SHEET

To be completed by the internal Data Protection Officer!

Date and time of the privacy incident:[5]

Organisational unit interfered by the privacy incident:

Circumstances relevant to the perception of the privacy incident:

Scope of personal data interfered by the privacy incident:

Scope and number of persons interfered by the privacy incident:

Description of the circumstances of the privacy incident:

Impacts of the privacy incident:

Description of the measures taken to prevent privacy incident:

Location, date

.....

internal data protection officer

4 Filed as appropriate, for instance 1/2017/AVINC, i.e. Incident No. 1 in year 2017.

5 From the date and time (day-hour-minute) of the incident until the date and time (day-hour-minute) of the final elimination of the incident.

Enclosure No. 22/2

NOTIFICATION LIST FOR PRIVACY INCIDENTS

I. Scope of private persons interfered by the privacy incident: (if data were lost, the path through which data at the redundant backup location were accessed should be inserted)

Name and contact data of the data subject:

1. .....
2. .....
3. .....
4. .....

II. Data of the organisation concerned and organisational data/scope of information interfered by the privacy incident: (if data were lost, the path through which data at the redundant backup location were accessed should be inserted)

Name, address, tax identifier and contact data of organisations concerned:

1. .....
2. .....
3. .....
4. .....

Notification order: notification of private persons concerned is of primary importance.

Date: .....

.....
signature
[Internal Data Protection Officer]

Enclosure No. 23

DATA PROCESSING CONTRACT

Data processing legal relationship established in accordance with Section II, Article 7 of Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and Point 18 of Section 3 of Act XCII of 2011 on the Right of Informational Self-Determination and Freedom of Information:

Name of data controller: .....
.....
Address: .....
Telephone: ..... fax..... e-mail: .....
(Data Controller)
and
Name of data processor: .....
.....
Address: .....
Telephone: ..... fax..... e-mail: .....
(Data Processor)

agree as follows: in due consideration of the provisions stipulated in this present contract, always ensuring the protection of personal data and fully respecting the right of self-determination of individual persons, as a basic right protected by the European Union as well as by the Member States, the Data Controller performs data processing procedures related to its activities as specified in this present contract, with the engagement of the Data Processor.

Article 1
Glossary

For the purpose of this present contract the terms **"personal data", "sensitive personal data", "data controlling/data controller", "data processing/data processor", "data subject"** are identical with the terms used in Act XCII of 2011 on the Right of Informational Self-Determination and Freedom of Information promulgated by the Hungarian National Assembly (hereinafter „Infotv."), and the terms used by Directive 95/46/EC of the European Parliament and the Council dated on 24 October 1995 (hereinafter „Directive").

Article 2
Details of data processing

Description of the data processing procedure of the Data Controller:
XxX
Tasks of the Data Processor in data controlling:
XxX
Scope of data subjects:
XxX
Scope of personal data processed:
XxX
Description of the activities of the Data Processor related to data controlling:
XxX

Article 3
Legislation and applicable law

The Data Controller is headquartered in Hungary and the data controlling is performed in Hungary in due consideration of Article 29 of the opinion No. 0836-02/10/HU WP 179 8/2010 of the data protection working group about the applicable law – the entire data controlling and any related procedures (specifically data processing) are subjected to the Hungarian law.

Article 4
Rights and obligations of the Data Processor and the Data Controller

Data Controller: The lawfulness of the instructions given to the Data Processor is the responsibility of the Data Controller. The Data Controller may give instructions to the Data Processor only in writing.

The Data Processor may engage further Data Processors in accordance with the instructions given by the Data Controller; such further Data Processors are named in Enclosure 1 of this present contract.

The Data Processor may not make in-merit decisions regarding data controlling, it may process personal data coming to its knowledge exclusively in accordance with the instructions received from the Data Controller, it may not process data for its own purposes, furthermore it is obliged to store and keep personal data in accordance with the instructions received from the Data Controller.

The Data Processor is obliged to observe the provisions stipulated in the Data Protection Regulation of the Data Controller, and to perform its tasks in connection with data controlling in accordance with the provisions stipulated therein.

The Data Processor is obliged to observe data security requirements in accordance with the provisions stipulated in the Data Protection Regulation of the Data Controller.

Article 5
Liability

If in the course of performing its tasks, the Data Processor acts in due consideration of the provisions stipulated in this present contract, then the Data Controller shall become liable for the activities of the Data Processor as for its own activities. If through its activities the Data Processor would cause any loss to the data subject or to a third person, the liability towards the data subject or the third person is burdened on the Data Controller.

If the Data Processor would transgress its rights specified in this present contract, in respect of such transgression it will become Data Controller and shall be liable towards the data subject or the third person for any loss caused in accordance with the general rules of wrongdoing.

Article 6
Mediation and competence

The parties hereby agree that they will settle any debate stemming from this present contract primarily amicably, through reconciliations and negotiations. If that would prove to be unsuccessful then they agree on the competence of on the High Court of Justice ..... or the ..... Court of Justice depending upon the value of the subject matter litigated.

Article 7
Cooperation with the data protection authorities

The parties hereby agree that they will submit a copy of this present contract to the data protection authorities designated according to their respective legal rules, provided that they are obliged to do so under their national laws.

Article 8
Closing provisions

This contract can be amended exclusively in writing with the official signature of person(s) entitled to undertake obligations.

The contracting parties after studying and interpreting this present contract and duly consenting its content in all aspects signed same affirmatively.

Article 9

On behalf of the Data Controller:
Name: .....
Title: .....

.....
signature
(official seal of the organisation)

On behalf of the Data Processor:
Name: .....
Title: .....

.....
signature
(official seal of the organisation)