DATA PROTECTION INFORMATION MATERIAL FOR PERSONS ENTERING THE COMPANY'S PREMISES

Security tasks in the facility are performed under service contract:

Safety Sector Limited liability company

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 Ltd.
corporate registration number:	Cg.06-09-015211
headquarters:	6728 Szeged, Wolfgang Sandner u. 3.
e-contact	Info@eli-alps.hu
represented by:	Dr. Gábor Szabó Managing Director
contact of data protection officer:	dataprotectionofficer@eli-alps.hu

Hereby we inform our visitors that the facility in Szeged (6728 Szeged, Wolfgang Sandner u. 3.) 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 which is located in the Company's area, but not operated by the Company, but an external firm. To enter into this area shall be authorized by the external entity.

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 Safety Sector Ltd. 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, the Company uses electronic surveillance system and electronic access control system in the premises of the facility. 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 Article 6 (1) Point a) of the GDPR with special regard to Section 2:48(1) of the Civil Code and the legal interest of the Company in accordance with Article 6(19) Point f) of the GDPR

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, 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, 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 Article 6 (1) Point a) of the GDPR with special regard to Section 2:48(1) of the Civil Code and the legal interest of the Company in accordance with Article 6(19) Point f) of the GDPR

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: electronically or 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: the legal interest of the Company in accordance with Article 6(1) Point f) of the GDPR
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 Wolfgang Sandner u. 3, Szeged 6728 with the legal basis and in accordance with the rules specified in Section 31 of the Szvtv. The cameras making up the system are owned by the Company, the Company takes care of safe storage of the recordings. The surveillance system is suitable for recording images.

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 three separate categories according to the aim of surveillance.

The first category is the so-called Sector I where the purpose of the surveillance is the safe storage, handling and transport of property and equipment, money, securities, precious metals and precious stones of at least significant value in accordance with the Act on Penal Code.

The second category is the so-called Sector II where the purpose of the surveillance is to guard hazardous substances.

The third category is the so-called Sector III where the legislation governing the applied electronic monitoring system is provided for in Article 6 (1) (f) of the GDPR and Section 6 of the Infotv. as the legitimate interest of the Company.

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

In the case of all three sectors, the application of the electronic monitoring system is exclusively for personal and property, fire and work protection purposes, and cannot be used to monitor the work intensity and private life of employees.

Recordings are automatically overwritten after 6 days. In this regard, the Company enables the data subjects for 6 days from the recording that if their right or legitimate interest is affected by the recording, they can request the data controller not to destroc or delete the data within the above-defined cancellation period (6 days). The request will be decided by the Company's data protection officer as soon as possible. The recording so marked shall be saved and handed over to the data protection officer, who shall ensure that it is properly guarded in accordance with its Privacy Policy in accordance with these Regulations. At the request of a court or other authority, the recording shall be sent to the court or authority without delay. If no request is made within thirty days of the request for non-destruction, the recording shall be deleted.

The data management information on the use of the electronic monitoring system used in Sectors I and II can be found in Enclosures 17 and 18 of the Data Protection Regulation.

Electronic monitoring in Sector III is subject to special rules, the related data management information is contained in Enclosure 19 of the Data Protection regulation.

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 within 6 days following the recording.

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 data protection officer).

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, equipment 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: consent of the data subject in accordance with Article 6(1) Point a) of the GDPR and §2:48(1) of the Act V of 2013 on the Civil Code

time scope of data storage:

- if the record is not utilised, it will be erased within 6 days passing from recording
- 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

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: consent of the data subject in accordance with Article 6(1) Point a) of the GDPR and §2:48(1) of the Act V of 2013 on the Civil Code

time scope of data storage:

- if the record is not utilised, it will be erased within 6 days passing from recording
- 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

method of data processing: electronically

Sector III

purpose of data processing: Continuous documentation of the assembly and installation and operation of the Company's research technology equipment and safe work, recording and use of recording of the assembly and installation process and operation and safe work so that it can be viewed at any time for the possible disassembly, reassembly, modification and safe operation of the equipment.

scope of processed data: Sound and image of the person(s) involved in the installation, other data that can be contacted with the person(s) involved.

legal ground of data processing: legal interest of the Company in accordance with Article 6(1) Point f) of the GDPR and §6 of the Infotv.

time scope of data storage: indefinite period of time

method of data processing: electronically

Enforcement of the rights of data subjects

Right to Information:

The data subject may request information on the processing of his / her personal data, as well as request the correction or deletion of his / her personal data at the contact details of the Company, with the exception of the data processing ordered by law.

The Company is obliged to forward the received application or protest to the head of the organizational unit responsible for data management within three days of receipt.

The head of the organizational unit with tasks and competencies shall respond to the request related to the processing of the personal data of the data subject in writing in a comprehensible form no later than 25 days - or 15 days in the case of exercising the right to protest.
If the assessment of the case is unclear during the exercise of the data subject's rights, the head of the data processing unit may request a resolution from the data protection officer by sending the case file and his/her position on the case, who shall comply with it within three days.

The notification covers the information specified in Article 15 (1) of the GDPR, insofar as the information of the data subject cannot be refused by law. The Company shall take appropriate measures to provide the data subject with all information concerning the processing of personal data referred to in Articles 13 and 14 of the GDPR and notification in accordance with Articles 15 to 22 and Article 34 of the GDPR shall be provided in a concise, transparent, comprehensible and easily accessible form, in a clear and comprehensible manner. The notification shall be provided in writing or by other means, including, where appropriate, by electronic means. Oral information may be provided at the request of the data subject, provided that the identity of the data subject has been otherwise established.

The notification is, in principle, free of charge, and the Company may charge a fee only in the case specified in Article 12 (5) (a) of the GDPR.

The Company shall reject the application only for the reasons specified in Article 12 (5) (b) of the GDPR, and this may only be done in writing, with due justification and appropriate information.

Right to Correction and Deletion (right to be forgotten):

Inaccurate data shall be corrected by the head of the department processing the data, if the necessary data and authenticating instruments proving them are available, and shall take steps to delete the processed personal data if the reasons set out in Article 17 of the GDPR exist.

The data subject shall have the right to request the deletion of the personal data concerning him without undue delay and the Company shall delete the personal data concerning him without undue delay, in particular if one of the following reasons exists:

- personal data are no longer required for the purpose for which they were collected or otherwise processed;
- the data subject withdraws his or her consent and there is no other legal basis for the processing;
- the data subject objects to the data processing and there is no overriding legitimate reason for the data processing or the data subject objects to the data processing for the direct acquisition of business;
- personal data have been processed unlawfully;
- personal data were collected in connection with the provision of information society services to children under the age of 16;
- if the Data Controller has disclosed the personal data and the personal data are no longer needed for the purpose for which they were collected or otherwise processed, it shall be deleted and the data controller shall take reasonable steps, taking into account the available technology and implementation costs, including technical measures to inform the controllers that the data subject has requested the deletion of links to the personal data in question or of a copy or duplicate of such personal data.

Protest against the management of personal data:

The data subject has the right to object to the processing of his / her personal data at any time by means of a declaration to the Company, in particular if the processing or transfer of personal data is necessary solely to fulfill a legal obligation to the Data Controller or a legitimate interest

of the Data Controller, except for mandatory data processing or if the use or transfer of personal data is for the purpose of direct business acquisition, public opinion polling or scientific research; and in other cases specified by law.

For the duration of the examination of the data subject's objection to the processing of personal data, but for a maximum of 5 days, the data controller shall suspend the processing, examine the validity of the objection and make a decision, informing the applicant in accordance with Article 19 of the GDPR.

If the objection is justified, the controller shall act in accordance with Article 21 of the GDPR.

If the Data Controller finds that the data subject's objection is justified, the data processing, including further data collection and data transfer, shall be terminated, the data shall be blocked and the protest and the measures taken on the basis thereof shall be notified to all persons to whom the personal data has been transmitted and so who are obliged to take measures to enforce the right to protest.

If the data subject does not agree with the decision of the Data Controller, or if the Data Controller fails to meet the deadline for replying, the data subject may apply to a court within 30 days from the notification of the decision or the last day of the deadline.

If the data recipient does not receive the data necessary for the exercise of the data subject's right due to the data subject's protest, he / she may apply to court against the Data Controller in 15 days from the service of the notification in order to obtain the data. The Data Controller may also sue the data subject.

If the Data Controller fails to notify, the Data Receiver may request information from the Data Controller regarding the circumstances related to the failure of the data transfer, which the Data Controller is obliged to provide within 8 days after the delivery of the Data Recipient's request. In the event of a request for information, the data recipient may turn to court against the Data Controller within 15 days of the provision of the information, but no later than within the open deadline. The Data Controller may also sue the data subject.

The Data Controller may not delete the data of the data subject if the data processing has been ordered by law. However, the data may not be transferred to the data recipient if the data controller has agreed to the protest or the court has established the legitimacy of the protest.

If the assessment of the case is unclear in the exercise of the data subject's rights, the head of the department handling the data may request a resolution from the Data Protection Officer by sending the case file and his / her position on the case, who shall comply with it within three days.

Right to restrict data processing:

The data subject has the right to request the Company to restrict the data processing if

- the data subject disputes the accuracy of the personal data (in this case, the restriction applies to the period of time that allows the Company to verify the accuracy of the personal data);
- the processing is unlawful and the data subject opposes the deletion of the data and instead requests that their use be restricted;
- the Company no longer needs personal data for the purpose of data processing, but the data subject requests it in order to submit, enforce or protect legal claims;
- the data processing is necessary for the performance of a task in the public interest or the data processing is necessary for the legitimate interests of the Company or a third party and the data subject has objected to the data processing for these purposes (in this case the restriction takes precedence over the legitimate reasons of the data subject).

Restriction of data management means that the Company does not process the personal data affected by the restriction, except for storage, or only to the extent to which the data subject has consented, or the Company may, in the absence of such consent, handle the data necessary to protect the rights of another natural or legal person or in the overriding public interest of the Union or of a Member State of the European Union. The Company informs the data subject in advance about the lifting of the data management restriction.

The Right to Data Portability:

In the course of the data management activities of the Company recorded in this privacy policy, no data management is carried out that would require the provision of data portability.

Automated Decision Making in Individual Cases, Including Profiling:

Automated decision-making does not take place during the Data Controller's data management.

Right to Compensation for Damage Caused by Unlawful Data Processing:

The data controller shall also reimburse the damage caused to others by the unlawful processing of the data subject's data and by the breach of data security requirements, furthermore the damages caused by the personal data breach by him or by the data processor used by data controller. The data controller shall be released from liability for the damage caused and the obligation to pay damages if he proves that the damage or the violation of the data subject's personal rights was caused by an unavoidable cause outside the scope of data processing. Likewise, it does not compensate for damage if it was caused by the intentional or grossly negligent conduct of the injured party.

Right to Legal Remedy:

The relevant legal remedy or complaint may be addressed by the data subject to the Company's data protection officer (Dr. Papp Viktória; dataprotectionofficer@eli-alps.hu; 6728 Szeged, Wolfgang Sandner u. 3.) directly or, at data subject's option, to the National Data Protection and Freedom of Information Authority (1055 Budapest, Falk Miksa utca 9-11; postal address: 1363 Budapest, Pf. 9.) or to the high court competent based on the place of residence or stay. In order to enforce the right to a judicial remedy, the data subject may, in the context of data processing operations falling within the scope of the data controller's activities, take legal action against the data controller if he considers that the data controller or the data controller acting on his behalf is in breach of the rules laid down in law or in a binding act of the European Union. The court is acting in expedited procedure in the case.