Data Protection Policy of Donauchem Vegyianyag Kereskedelmi Kft

Based on Act XCII of 2011 on the Right of Informational Self-Determination and on Freedom of Information (hereinafter referred to as Data Protection Act), as well as Act CXXXIII of 2005 on Security Services and the Activities of Private Investigators, Donauchem Vegyianyag Kereskedelmi Kft (hereinafter referred to as Organization) shall formulate the following policy concerning data protection, data security and data processing operations. The processing of personal data by the Organization may also be regulated by other industry specific rules, which are also respected by the Organization during its data processing operations and which were taken into account when this Policy was drafted.

Article 1 Purpose of Scope of the Policy

(1) Under Article VI of the Fundamental Law of Hungary, everyone has the right to the protection of personal data concerning him, and access to data of public interest. The exercise of the right to the protection of personal data and access to data of public interest shall be supervised by an independent authority established by the state. This authority is the Hungarian National Authority for Data Protection and Freedom of Information (hereinafter referred to as NAIH).

(2) Donauchem Vegyianyag Kereskedelmi Kft stresses the importance of the protection of personal data and the confidential processing thereof, as well as the disclosure of data of public interest and data public on grounds of public interest. The Data Protection Policy of the Organization (hereinafter referred to as Policy) contains the most important data protection rules and principles concerning the records kept by the Organization, with special regard to the requirements related to data handling, data processing, data transmission, data protection and disclosure. The purpose of the Policy is to determine the conditions and method of processing data relating to the operation of the Organization in accordance with the relevant rules of law, respecting the interests of the society and the data subjects.

(3) The purpose of this Policy is to determine the statutory order of the records kept by the Organization, to ensure the enforcement of the constitutional principles of data protection, the right of informational self-determination and data security requirements, and to prevent unauthorized access to, as well as unauthorized change or disclosure of the data.

(4) The scope ratione personae of this Policy shall extend to all persons having an employment, contractual or other relationship aiming at the performance of work with the Organization.

(5) The scope ratione personae of this Policy shall also extend to those people who do not have any of the above-mentioned relationships with the Organization, however

a) the Organization processes their data in order to create such a legal relationship,
b) the Organization is obliged to process their data upon the termination of the legal

relationship due to the legal requirements.

(6) The material scope of this Policy shall cover all personal information, data of public interest and data public on grounds of public interest processed by the Organization pursuant to the regulations.

(7) The scope of this Policy shall not extend to technical data protection connected to IT devices, which is subject to the Information Security Policy.

Article 2 Definitions

In addition to the definitions set forth in the Data Protection Act, the following terms shall have the following meaning in this Policy:

(1) **data subject:** a natural person who has been identified by reference to specific personal data, or who can be identified, directly or indirectly;

(2) **personal data:** data relating to the data subject, in particular by reference to the name and identification number of the data subject or one or more factors specific to his physical, physiological, mental, economic, cultural or social identity as well as conclusions drawn from the data in regard to the data subject;

(3) **consent:** any freely and expressly given specific and informed indication of the will of the data subject by which he signifies his agreement to personal data relating to him being processed fully or to the extent of specific operations;

(4) **objection:** a declaration made by the data subject objecting to the processing of their personal data and requesting the termination of data processing, as well as the erasure of the data processed;

(5) **data protection:** statutory regulation concerning the processing of personal and sensitive data in order to exercise the data subject's right to informational self-determination;

(6) **right to informational self-determination:** the content of the right to the protection of personal data provided for by Article VI of the Fundamental Law, according to which everybody has the right to decide on the disclosure and use of their personal data;

(7) **controller:** a natural person or legal entity or organisation without legal personality which, alone or jointly with others, determines the purposes and means of the processing of personal data, makes and implements relevant decisions (including those related to the tools used) or delegates them to the respective appointed data processor;

(8) **data processing:** any operation or the totality of operations performed on the data, irrespective of the procedure applied; in particular, collecting, recording, registering, classifying, storing, modifying, using, querying, transferring, disclosing, synchronising or connecting, blocking, deleting and destructing the data, as well as preventing their further use, taking photos, making audio or visual recordings, as well as registering physical characteristics suitable for personal identification (such as fingerprints or palm prints, DNA samples, iris scans);

(9) **data transfer:** ensuring access to the data for a third party;

(10) **disclosure:** ensuring open access to the data;

(11) **data deletion:** making data unrecognisable in a way that it can never again be restored;

(12) **tagging data:** marking data with a special ID tag to differentiate it;

(13) **blocking of data:** marking data with a special ID tag to indefinitely or definitely restrict its further processing;

(14) **data destruction:** complete physical destruction of the data carrier recording the data;

(15) **data process:** performing technical tasks in connection with data processing operations, irrespective of the method and means used for executing the operations, as well as the place of execution, provided that the technical task is performed on the data;

(16) **data processor:** any natural or legal person or organisation without legal personality processing the data on the grounds of a contract, including contracts concluded pursuant to legislative provisions;

(17) **data source:** the body responsible for undertaking the public responsibility which generated the data of public interest that must be disclosed through electronic means, or during the course of operation in which this data was generated;

(18) **data disseminator:** the body responsible for undertaking the public responsibility which uploads the data sent by the data source, if the data have not published by the data source;

(19) **data set:** all data processed in a single file;

(20) **third party**: any natural or legal person, or organisation without legal personality other than the data subject, the data controller or the data processor.

(21) **data security:** a set of organizational, technical solutions and procedural rules against the unauthorized processing of personal data, in particular the acquisition, processing, alteration and destruction of personal data; the state of data management in which the risk factors – and thus the threat – are reduced to the smallest by the organization, technical solutions and measures;

(22) **data owner:** head of the authorities, or any person who is entitled to make a decision concerning the specific data processing;

(23) **the right of access and the right to know**: a data subject shall have the right of access to personal and sensitive data that have been collected concerning him, and to know such data;

(24) **direct right of access:** a data subject shall have the right of access to the data of a specific data set processed with an information technology application, which enables the data subject to directly retrieve the processed data at a time selected thereby;

(25) **direct retrieval:** data subject shall have the right of access to data processed in a specific data set – by using the general right to search made previously available by the controller – at a date and time not specified previously, which access shall be recorded in a log, as well as the right to print or record such information in any other way;

(26) **data carrier:** any material – containing personal or sensitive data – generated in any form, by using any tool and any procedure;

(27) **hardware:** any device that ensures the continuous operation of the information technology system, or which serves to make data backup or copies, and which provides protection for the computer against external influences electronically or in another manner;

(28) **means of communication:** any technical tool or technological procedure that is suitable for receiving or transmitting signals, data and information to one or more recipients;

(29) **data incident:** a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

Article 3 Data protection, data security and data processing organization

(1) The heads of the organizational units shall ensure compliance with and enforcement of the content of this Policy.

(2) Our contractual partner, A12 Lap Kft, shall be responsible for the technical protection of the information technology devices in accordance with the Information Security Policy.

Article 4 Data Protection Officer

(1) If necessary, the Managing Director shall designate the Data Protection Officer of the organization.

(2) The Data Protection Officer of our organization is: Szilvia Gazdag, her contact details are as follows: iroda@donauchem.hu / telephone number: +36 1 207-8000.

(3) The Data Protection Officer shall keep the following records:

a) She shall keep records to control measures relating to the data incident and to inform data subjects, containing the personal data affected, the personal scope affected by the data incident, the time, circumstances and effects of the data incident and measures taken to eliminate thereof as well as other information specified in the regulation prescribing the data processing operation, in accordance with Schedule 1 to this Policy;

b) She shall keep records on data transfers to control the legality of data transfers and to inform data subjects, containing the time of transferring personal data processed thereby, the grounds and addressee of data transfer, the scope of personal data transferred, as well as other information specified in the regulation prescribing the data processing operation, in accordance with Schedule 2 to this Policy;

(4) In addition to what is contained in Section (2) above, the Data Protection Officer shall

a) participate in and provide assistance to make decisions connected to data processing, and ensure the rights of data subjects;

b) monitor compliance with the Data Protection Act and other data protection provisions, as well as the provisions and data security requirements of the internal policies in relation to the protection of personal data;

c) examine the reporting by natural persons, and in case of observing unauthorized data processing, she shall call on the controller or data processor to cease such unauthorized data processing;

d) prepare the internal data protection information;

e) provide training on information concerning data protection;

f) prepare the application for the registration of data processing to be reported to the authorities, and submit such applications.

Article 5 Principles of data protection

(1) Personal or sensitive data processed must be essential for the purpose for which it was recorded, and it must be suitable to achieve that purpose. Personal or sensitive data may be processed to the extent and for the duration necessary to achieve its purpose.

(2) The employees and external contractors (hereinafter referred to as Employees) may only process personal and sensitive data in the exercise of their tasks by respecting the provisions of the relevant legislation.

(3) Pursuant to the Fundamental Law, which ensures the right of informational self-determination of data subjects, every natural person shall have the right to the protection of his personal data. The right of informational self-determination may only be restricted based on authorization conferred by law in the absence of the consent of data subjects. In order to respect the right of informational self-determination the Employees of controller may only process personal data in cases provided for by the law, or if – in accordance with the law – the head of the controller orders it, or the data subject expressly has consented to it (which has to be made in writing in case of sensitive data).

(4) The employee of controller processing data shall have disciplinary, damages, administrative and criminal law liability for the legal processing of personal data became known to him or in the performance of his duties and for the exercise of his functions, and for the legal exercise of the rights of access to the records of the controller.

(5) Personal data may be processed only for specified and explicit purposes, where it is necessary for the exercising of certain rights and fulfilment of obligations. In case of data processing ordered by the law, data may only be processed for the purpose specified in the law providing the authorization. Personal data processed by the controller – or made available by another controller to perform the duties of controller – may not be used for private purposes. The data processing shall satisfy the principle of purpose limitation.

(6) If the Employee of the controller becomes aware of the fact that the personal data processed thereby is inaccurate, incomplete or outdated, the Employee shall correct such data or request the correction thereof from the employee in charge of recording the data.

(7) Personal data may only be processed,

a) when the data subject has given his consent, or

b) when processing is necessary as decreed by law or by a local authority - based on authorization conferred by law - for the performance of a task carried out in the public interest (mandatory processing).

(8) Personal data may also be processed if obtaining the data subject's consent is impossible or it would give rise to disproportionate costs, and the processing of personal data is necessary

a) for compliance with a legal obligation pertaining to the data controller, or

b) for the purposes of the legitimate interest pursued by the controller or a third party, and enforcing these interests is considered proportionate to the limitation of the right for the protection of personal data.

(9) Where personal data is recorded under the data subject's consent, the controller shall – unless otherwise provided for by law – be able to process the data recorded where this is necessary

a) for compliance with a legal obligation pertaining to the data controller, or

b) for the purposes of the legitimate interest pursued by the controller or a third party, and enforcing these interests is considered proportionate to the limitation of the right for the protection of personal data, without the data subject's further consent, or after the data subject having withdrawn his consent.

(10) Personal data may only be processed based on the informed consent of the data subject.

(11) The accuracy and completeness, and – if deemed necessary in the light of the aim of processing – the up-to-dateness of the data must be provided for throughout the processing operation, and shall be kept in a way to permit the identification of the data subject for no longer than is necessary for the purposes for which the data were recorded. The controller may be contacted by any court, prosecutor's office, investigative authority, administrative authority, the Hungarian National Authority for Data Protection and Freedom of Information, and other public bodies based on authorization conferred by law to provide, disclose or hand over information, or to make documents available. The controller shall provide the authorities with the requested information if the exact purpose and the scope of data have been indicated by the authority. However, personal data may only be provided to the extent necessary for the purpose of the request.

Article 6 Principles of data processing

(1) Protection of personal data: Personal data may be processed when the data subject has given his consent, or when processing is necessary as decreed by law. Personal data may be processed also if obtaining the data subject's consent is impossible or it would give rise to disproportionate costs, and the processing of personal data is necessary for compliance with a legal obligation pertaining to the Organization, or for the purposes of legitimate interests pursued by the Organization or by a third party. Unintentionally disclosed data are not stored or transmitted by the Organization.

(2) Purpose limitation and proportionality of data processing: The Organization may only process personal data for a specific purpose, to exercise a right or to fulfil an obligation.

(3) Principle of data quality: The Organization shall record and process personal data lawfully and fairly. The data shall be accurate, complete and up to date, and kept in a form which permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

(4) Protection of sensitive data: Sensitive data may only be processed by the Organization

a) when the data subject has given his consent in writing, or

b) when processing is necessary for the implementation of an international agreement, if prescribed by law in connection with the enforcement of fundamental rights afforded by the Fundamental Law, or for reasons of national security, or law enforcement purposes for the prevention or prosecution of criminal activities, or

c) it is prescribed by law in other cases.

(5) Protection of data constituting trade secret: Trade secret has to be protected. Any data

qualified as trade secret by the Organization or the business partner thereof may not be disclosed to any third party, unless:

a) the business partner has consented to it previously in writing,

b) it is requested by the authority or the court,

c) the data is of public interest or data public on grounds of public interest,

d) it has to be disclosed for other reasons based on a regulation.

(6) Data security: The Organization shall make arrangements for and carry out data processing operations in a way so as to protect the data.

(7) Information of the data subject: Prior to recording the data, the data subject shall be informed whether his consent is required or processing is mandatory. In case of mandatory data supply the legislation ordering the data processing shall also be indicated.

Article 7 Scope of data handled and processed in the documents of the Organization

(1) Scope of personal data: Documents containing personal data specified by the Data Protection Act processed by the Organization as an employer concerning its employees.

(2) Scope of data constituting trade secret: trade secret is a fact, information, other data or the compilation of these, related to commercial activity, not generally known among or readily accessible to persons performing the affected commercial activity, the unlawful acquisition, use and disclosure or publication of which would harm or jeopardise the legitimate financial, economic or market interest of the data subject, provided that it has been subject to reasonable steps under the circumstances by the lawful beneficiary of the information to keep it secret. Know-how, being a technical, economic and organizational knowledge, solution, experience and any combination thereof held in a form enabling identification, also qualifies as trade secret. In particular, it includes data related to technology, technical solutions, production processes, work organization, and logistic methods. Any other data considered as trade secret by the business partner in its relationship with the Organization shall be deemed as trade secret.

(3) Data of public interest: In the course of the operation of the Organization, it refers to data that are in public interest based on the legislation, and the tender documents processed during the management of tenders, with the exception of personal data. There is a separate policy concerning the access to data of public interest.

(4) Data public on grounds of public interest: In the course of the operation of the Organization and performing its tasks related to the management of tenders, it refers to data that are public on grounds of public interest specified by rules of law.

(5) Sensitive data: Sensitive data appearing in tender documents and personal files during the operation of the Organization.

(6) Tender documents: data carrier related to the tender managed by the Organization partly or wholly, generated on any material, in any form and with the use of any device, which contains any data in connection with the tender or the tenderers.

(7) With regard to the content of this Policy, the provisions of separate regulations may

provide for the data processed by a given organizational unit of the Organization. This Policy shall apply to the data not regulated by the separate regulations. The separate regulations may not deviate from the provisions of the Data Protection Act.

Article 8 Measures necessary for the protection of personal data

(1) Controller shall make arrangements for and carry out data processing operations in a way so as to ensure full respect for the right to privacy of data subjects.

(2) Any person having a legal relationship with the Organization under Article 1 (4) of this Policy (hereinafter referred to as people having a legal relationship with the Organization), who becomes aware of personal data, processes such data based on his position or function, shall store and safeguard the personal data and make every effort to ensure their adequate protection. Data shall be protected by means of suitable measures against unauthorized access, alteration, transmission, public disclosure, deletion or destruction, as well as damage and accidental loss, and to ensure that stored data cannot be corrupted and rendered inaccessible due to any changes in or modification to the applied technique.

(3) Where the person having a legal relationship with the Organization has an access to or becomes aware of personal, sensitive or criminal data due to his position or function, he shall act in accordance with the provisions of the Data Protection Act, thus, in particular, he may only use the personal data for the pre-determined purpose, and the data shall be protected from unauthorised access.

(4) The people having a legal relationship with the Organization shall be liable for any damage arising from the violation of their data processing, data protection obligation specified herein.

(5) Where the Organization establishes a contractual relationship with any third party aiming at the performance of an activity other than processing data, in the course of which personal data are processed, the contract shall include the obligation to respect the provisions of the relevant rules of law, this Policy and the Information Security Policy.

(6) Controller, and within their sphere of competence, data processors must implement adequate safeguards and appropriate technical and organizational measures to protect personal data, as well as adequate procedural rules to enforce the provisions of the law and this Policy.

(7) In determining the measures to ensure security of processing, data controllers and processors shall proceed taking into account the latest technical development and the state of the art of their implementation, except if this would entail unreasonable hardship for the data controller.

(8) In respect of automated personal data processing, data controllers and processors shall implement additional measures designed to:

a) prevent the unauthorized entry of data;

b) prevent the use of automated data-processing systems by unauthorized persons using data transfer devices;

c) ensure that it is possible to verify and establish to which bodies personal data have

been or may be transmitted or made available using data transfer devices;

d) ensure that it is possible to verify and establish which personal data have been entered into automated data-processing systems and when and by whom the data were input;

e) ensure that installed systems may, in case of malfunctions, be restored, and

f) ensure that faults emerging in automated data-processing systems is reported.

(9) The service provider developing the information technology system is responsible for logging the problems of the IT system arising in the course of automated data processing, and providing the opportunity for such logging.

Article 9 Information

(1) Prior to data processing being initiated the data subject shall be informed whether his consent is required or processing is mandatory. Before processing operations are carried out, the data subject shall be clearly and elaborately informed of all aspects concerning the processing of his personal data, such as the purpose for which his data is required and the legal basis, the person entitled to control the data and to carry out the processing, the duration of the proposed processing operation, if the data subject's personal data is processed by the controller with data subject's consent, in order to satisfy an obligation of the controller or to enforce the legitimate interest of a third party, and the persons to whom his data may be disclosed.

(2) Information shall also be provided on the data subject's rights and remedies. The information under Section (1) shall be provided

a) with the content specified in Schedule 3 to this Policy when the legal relationship is established with the Organization, within the scope of providing general information,

b) with the content specified in Schedule 4 to this Policy when contractual or other legal relationship aimed at the performance of work is established with the Organization,

c) with the content specified in Schedule 5 to this Policy in the job advertisement for people submitting their application to the Organization.

(3) The information provided under Section (2) shall be placed on the website of the Organization or shall be made available in the administrative centre of the Organization.

(4) The information provided under Section (2)

a) paragraph a) shall be made available on paper or electronically,

b) paragraph b) shall be incorporated into the wording of the contract,

c) paragraph c) shall be made available in the job advertisement with reference to the website address mentioned in Section (3), by indicating the path precisely, at least in the Hungarian language.

Article 10 Data transfer within the Organization, linking data processing

(1) Within the organizational system of the Organization, personal data may only be transferred - to the extent and for the duration necessary to perform the task - to an organization unit or person that needs to become aware of and process the personal data in order to perform the activities specified in the legislation or in the

Organizational Policy.

(2) The processing of data having different purposes may only be linked in justified cases in accordance with the legitimate purposes.

Article 11 Data transfer based on request, data transfer to outside the organization

(1) Any request aiming at the transfer of personal data processed by the Organization may only be satisfied in accordance with the legal provisions or in case of the existence of the conditions set forth in Section (2). In any other cases the performance of data transfer must be refused.

(2) In cases when data transfer is not based on a legal obligation, it may only be performed if the data subject has given his express consent for it to the Organization. The data subject may also grant such a consent previously, which may be issued for a certain period of time or for a specific set of requesting bodies.

(3) The data subject may also grant such a consent previously, which may be issued for a certain period of time and/or for a specific set of requesting bodies. In this sense

a) bodies performing payroll accounting, or keeping employment records,

b) the representatives of the owner of the Organization,

c) the auditor, alternate auditor and

d) the external contracted sub-contractors, e.g. company doctor, workplace safety officer

shall be deemed as bodies outside the organization.

(4) Notwithstanding the declaration of the data subject, a request arriving from the authorities (police, court, prosecutor's office, tax authority, etc.) as well as the national security services shall be executed. The data concerning the request arriving from the national security services – under Act CLV of 2009 on the Protection of Classified Information – shall be classified information. The data may only be provided with the approval of the Managing Director or the Deputy Managing Director, and no other person or body may be informed about such data transfer.

(5) Data that are – under the relevant regulations - public, or have been made public for other reasons may be disclosed on request.

(6) Data supply based on the regulations is mandatory, and it is the responsibility of the competent organizational units to perform such data supply.

(7) Only the Managing Director or Deputy Managing Director may allow or order the performance of data supply based on consent. (Data requested by bodies other than the courts or authorities, e.g. an organization intends to compile a regional or national information booklet and requests data for it.)

(8) The Organization shall provide information on the data processed thereby in connection with the employee, and give a copy or an extract of the documents containing the processed data – on request – to the employee.

Article 12 Data transfer to other countries

(1) In case of data transfers to other countries the person performing the data transfer

shall ensure that the conditions of data transfer to other countries specified in the Data Protection Act exist. With regard to this it must be examined whether the data transfer takes place on the grounds specified in the Data Protection Act, and the adequate level of protection of the personal data have been ensured by the controller receiving the data. Transfer of data to EEA Member States shall be considered as if the transmission took place within the territory of Hungary.

Article 13 Data transfer for statistical purpose

(2) The Organization undertakes to transfer personal data for statistical purpose by ensuring that they may not be linked to the data subject.

Article 14 Processing personal data

(1) In the event the data may not be processed by the controller, an external organization may also be mandated to process data. The general rules of contracting and public procurement shall apply to contracts aiming at the processing of data. No organization that is interested in a business activity using the personal data to be processed may be mandated to process the data.

(2) The data processor under Section (1) may employ additional data processors in accordance with the instructions of the Organization.

Article 15 Recording of personal data

(1) The legal basis of data processing to document facts concerning the employment relationship are provided by Act I of 2012 on the Labour Code and the implementing regulations thereof.

(2) The data coming from employee records may be used for establishing facts related to the employment relationship of the employees, verifying classification requirements, supplying data for statistical purpose, and for administration connected to contracts related to employment.

(3) The employee records contain the personal data of all the employees of the Organization specified in Section (2).

(4) The data included in the employee records are provided by the data subject.

(5) The employee records are managed in the integrated HR module of the information technology department and on paper.

Article 16 Wages and employment records

(1) The provisions concerning employee records shall apply to the wages and employment records with the differences provided for in this section.

(2) The data coming from the wages and employment records may be used for establishing facts related to the legal relationship of the employee, verifying classification requirements, payroll accounting, social insurance administration and for statistical purposes.

Article 17 Measures taken in order to protect data generated in the course of the operation

(1) The staff of the Organization shall handle all the data, information or documents, etc.– irrespective of how and in what form they were obtained – which became known to them during the performance of their tasks or in connection therewith confidentially.

Article 18 Duration of the processing operation, deletion of data

(1) Duration of the processing operation:

In case of personal data

e) specified in the act on the rules of taxation,

f) specified in the act on eligibility for social security benefits and the coverage thereof

g) specified in the act on health insurance, it is the last day of the 6th year following the termination of the employment relationship, unless the legislation provides for a longer retention period;

In case of personal data

h) specified in the regulation providing for the mandatory use of journey logs and

i) specified in the regulation providing for the mandatory use of tachographs used in road traffic, it is the last day of the 5th year following the recording of the data, unless the legislation provides for a longer retention period;

j) in other cases the data is processed until the purpose of data processing is achieved, unless the legislation provides for a different retention period. The detailed rules concerning the retention of these data are explained in the policies providing for the other data processing of the Organization.

(2) Controller shall process the data from the moment they are made available until they are deleted. Personal data must be deleted if:

a) they have been unlawfully processed

b) the data are incomplete or incorrect, and this status may not be lawfully corrected, provided that the deletion is not excluded by the legislation

c) the purpose of data processing does not exist anymore

d) in case of data supply based on consent, if the data subject requests the deletion of his data

e) it has been ordered by the court or the data protection authority.

(3) Following the termination of the processing of personal data the document containing the personal data shall be moved to the archives, and it must be discarded or destroyed in accordance with the Document Management Policy in force and upon the expiration of the retention period specified by law.

Article 19 Confidentiality

(1) Any person having a legal relationship with the Organization shall store and safeguard all the data, information and documents that became known to them in the course of or in connection with the performance of their tasks arising from their position, the

contracts concluded with them, or their function, and shall make every effort to ensure their adequate protection.

(2) In order to satisfy their obligation specified in Section (1) the people having a legal relationship with the Organization shall ensure the handling and storing of intellectual product, research result, course material, invention, etc. mainly by means of organizational tools, or in case of organizational information technology services through an approved SLA. If such material is processed outside the Organization, they must ensure that the provisions of this Policy and other detailing policies may be enforced.

(3) Any person having a legal relationship with the Organization shall be liable for damages arising from the violation of their obligation concerning the processing of data or confidentiality outlined in Sections (1) and (2).

Article 20 Mandatory data protection registers

(1) Pursuant to the Data Protection Act, the Organization shall maintain the following registers:

a) Internal data protection register (Section 24 (1) (e) of the Data Protection Act)

b) Transmission log (Section 15 (2) of the Data Protection Act)

c) Records containing the personal data affected (Section 15 (1a) of the Data Protection Act)

d) Records on the requests for access to data of public interest refused (Section 30 (3) of the Data Protection Act)

(2) *Data protection register (official records)*

NAIH – on the basis of a previous request and reporting – shall maintain official records on the processing operations of controllers in respect of personal data (hereinafter referred to as Data Protection Register) for the purpose of providing assistance to data subjects. The Register is open to the public and anyone may inspect it. The Data Protection Register includes the following information:

a) the purpose of data processing,

b) the legal basis of data processing,

c) the scope of data subjects,

d) description of the data pertaining to the data subjects,

e) the source of data,

f) the duration of processing,

g) the categories of data transferred, the recipients and the grounds for transfer, including transfers made to third countries,

h) the name and address of the data controller and the data processor, the place where records are kept and where processing is carried out, and the data professor's activities in connection with the data processing operations,

i) the nature of the data process technology used,

j) the name and contact details of the internal data protection officer, where applicable.

(3) The reporting obligation shall apply to both mandatory data processing operations and data processing operations based on consent. In terms of registration, data controls with alternative objectives qualify as independent data controls even if the same set of data is controlled.

(4) The reporting shall be initiated – at the legal representative of the Organization – by the organizational unit where the data processing operations concerning personal data occurred. The reporting shall be done centrally.

(5) Concerning data falling within the scope of interest of the Organization, the authority's data protection register shall not cover operations concerning the data of data controller's

a) employees,

b) members,

c) students under student agreement or

d) customers.

(6) Where the processing of personal data exceeds the additional scope of data specified above and in Section 65 of the Data Protection Act, it may only be performed if the data processing was requested previously by the Organization from the Authority.

(7) *Internal data protection register*

The Organization – by means of a legal representative – shall keep records of data processing operations registered with the Authority.

(8) *Transmission log*

With a view to verifying legitimacy of data transfer and for the information of the data subject, the Organization – by means of a legal representative – shall maintain a transmission log with a content specified in Schedule 2 to this Policy.

(9) The duration of retention of the data concerning the central transmission log shall not be less than five years in respect of personal data, and twenty years in respect of special data.

(10) No records shall be maintained on the transfer of data within the Organization that is based on a legal provision or authorization and the description of the specific business process is necessary for the performance of intended work.

(11) *Records containing the personal data affected*

With a view to control measures relating to data incidents and to inform data subjects, the Organization – by means of a legal representative – shall keep records with data content specified in Schedule 1 to this Policy.

(12) *Records on the requests for access to data of public interest refused*

The Organization – by means of a legal representative – shall keep records on refused requests, as well as the grounds for refusal, and notify NAIH of the refused requests by 31 January of the following year.

Article 21 Rights of data subjects, enforcement

(1) In accordance with the provisions of the Data Protection Act and this Policy, the Data Protection Officer shall prepare information as to the rights of the data subject and

what to do in the event such rights are violated, including the possibilities for seeking judicial remedy or lodging a complaint with NAIH. This information shall be placed on the website of the Organization, and the path to the website must be indicated in the information specified in Article 9 (3) of this Policy.

(2) The data subject may request form the data controller information on his personal data being processed, and may inspect it following the verification of his entitlement. Such inspection must be ensured in a way that the data subject may not become aware of the personal data of other people.

(3) Upon the data subject's request the data controller shall provide information concerning the data relating to him, the sources from where they were obtained, the purpose, grounds and duration of processing, the conditions and effects of the data incident and measures taken with a view to eliminate them, and the legal basis and the recipients. Data controller must provide the information requested in an intelligible form, in writing at the data subject's request, within not more than 8 days following the receipt of the request.

(4) Should the data change or the data subject observe incorrect data recording, the data subject may request the rectification or correction of the data processed on him, or the erasure or blocking of his personal data, save where processing is rendered mandatory. Data controller must make the necessary changes, or correct the incorrect data and inform the data subject about the occurrence thereof without undue delay, but not later than within 8 working days following the receipt of the request.

(5) In the event the rights of data subject concerning data processing operations are violated, the data subject may turn to the Data Protection Officer, who shall investigate the request conveyed to him, and, if he detects any unauthorized data processing operations, calls on the head of the Organization to cease such operations. If the Organization refuses to comply with the data subject's request, the factual or legal reasons on which the decision for refusing the request is based shall be communicated in writing within 30 days of receipt of the request. Where the request is refused, the data controller shall inform the data subject of the possibilities for seeking judicial remedy or lodging a complaint with the authority.

(6) Data controller shall take minutes on the transfer of data performed on request as well as the refused requests. The minutes shall be taken in accordance with Schedule 2. The first copy of the minutes shall be kept at the location of data processing, and the second copy including its annexes shall be forwarded (in the event a copy is sent, the words "certified true copy" must be written on it and it must be stamped) to the Data Protection Officer, who shall notify the authority of the refused requests by 31 January of the following year. The minutes shall be stored for a period of five years.

Article 22 Measures related to data incidents

(1) Data controller shall keep records of data incidents occurring at the controller or at the data processor mandated by the controller. The data content of the records shall be in accordance with Schedule 1.

(2) The measures and communications related to data incidents are included in the Incident Management and Communications Policy of the Organization.

Article 23 General rules

(1) The Organization shall make arrangements for and carry out data processing operations in a way to ensure full respect for the right to privacy of data subjects in due compliance with the provisions of the Data Protection Act and other regulations on data protection.

(2) The Organization must implement adequate safeguards and appropriate technical and organizational measures to protect personal data, as well as adequate procedural rules to enforce the provisions of the Data Protection Act, and other regulations concerning confidentiality and security of data processing.

(3) In determining the measures to ensure security of processing, the Organization shall proceed taking into account the latest technical developments and the state of the art of their implementation. Where alternate data processing solutions are available, the one selected shall ensure the highest level of protection of personal data, except if this would entail unreasonable hardship for the data controller.

(4) Data must be protected by means of suitable measures against unauthorized access, alteration, transmission, public disclosure, deletion or destruction, as well as damage and accidental loss, and to ensure that stored data cannot be corrupted and rendered inaccessible due to any changes in or modification of the applied technique.

(5) In order to enforce regulations on data security, the necessary measures must be taken to ensure the security of personal data that are processed manually, or stored and processed on the computer.

Article 24 Data stored on a computer

(1) The Information Security Policy provides for the protection of data stored on computer.

Article 25 Data processed manually

(1) In order to ensure the security of personal data processed manually, the following measures must be taken:

a) documents deposited in archive must be placed in a dry room that can be locked and it has to be supplied with fire protection and security equipment;

b) only the competent officers may access documents that are processed continuously, documents related to personnel, wages and the employment relationship must be locked away safely,

c) the documents affected by the data processing operations specified in this Policy must be archived once a year, the archived documents must be sorted out and handled in accordance with the Document Management and Disposal Policy, as

well as the archive plans.

(2) The access procedure to the keys of the rooms and lockers as per Section (1) sub-section (b) shall be drafted by the head of the data processing organizational unit, and sent to the Data Protection Officer.

Article 26 Closing provisions

(1) This Policy shall come into force – except what is contained in Section (2) – on 25 May 2018.

At Budapest, on 25 May 2018.

……

Managing Director