SPORTMARKETING COMPANY Ltd.
DATA MANAGEMENT AND PRIVACY POLICY

Date of entry into force:
09 August 2022.

.....
Balázs Árpád Szalay
Managing Director

Table of contents

Preambulum

The Sportmarketing Agency Ltd. (hereinafter referred to as the "Controller" or the "Company") attaches great importance to respecting the right to information self-determination of its employees, partners, customers and visitors. The Company is subject to the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter referred to as the "Regulation" or "GDPR") and the 2011 Act on the Right to Information Self-Determination and Freedom of Information (hereinafter referred to as the "Act" or "Act"). In order to comply with the provisions of Act CXII of 2011 on the Freedom of Information and Access to Information and Data Protection (hereinafter referred to as "the GDPR") and to regulate data protection and data security, the following Data Protection Policy (hereinafter referred to as "the Privacy Policy", "the Policy") is hereby adopted, also with regard to Article 24 of the Regulation.

Controller's data:	
company name:	Sportmarketing Agency Ltd.
company registration number :	01-09-287952
is based in:	1065 Budapest, Podmaniczky utca 12. fszt. 3.
postacíme:	1065 Budapest, Podmaniczky utca 12. fszt. 3.
your electronic address:	info@dakar.hu
website address:	http://sportugynokseg.hu/
representative:	Balázs Árpád Szalay Managing Director
data protection relationship:	gdpr@sportugynokseg.hu

I. INTRODUCTORY PROVISIONS

I.1. Purpose of the Rules

1. The protection of natural persons with regard to the processing of their personal data is a fundamental right.

2. This Policy is intended to comply with the legal provisions governing data processing activities, in particular the following legal provisions:

a) GDPR
b) Infotv.

The purpose of this Policy is for the Controller to define the rules governing the handling, transmission, processing and protection of personal data processed in the context of its operations, the duties and powers of the departments (if the Company is divided into departments) and employees involved in the processing of personal data, and the responsibilities for the processing of personal data.

I.2. Scope of the Rules

4. The personal scope of the Policy extends to all employees of the Company, persons who have a contractual or other relationship with the Company, persons who carry out data processing or data handling activities, or persons who have access to personal data processed by the Company.

5. The scope of the Policy covers all processes involving the processing of personal data by the Controller, regardless of the processing method, and the personal data processed by the Controller. In addition, the scope of this Policy extends to data transfers and exchanges of personal data (including processing activities in the context of joint processing) with processors, other controllers, supervisory authorities, other public authorities or any other third parties. The processing activities of the Company as a processor are covered by this Policy only where such a provision of the processing agreement so provides, to the extent provided.

6. These Regulations and the provisions contained therein shall enter into force on 09 August 2022.

7. The provisions of this Policy shall be interpreted in accordance with the provisions of the other policies of the Controller. In the event of any conflict between the provisions of this Policy and the provisions of other policies of the Controller with regard to the processing or protection of personal data, the provisions of this Policy shall apply.

I.3. Interpretative provisions

8. The conceptual system of the Rules corresponds to the conceptual system defined in Article 4 of the Regulation and in Article 3 of the Infotv.

9. Where the definitions in the applicable data protection legislation differ from the definitions in the Policy, the definitions in the legislation shall prevail.

10. Where the Policy or any other document of the Controller governing the processing of personal data refers to processing or data, it shall be understood as processing of personal data or personal data, unless otherwise stated.

11. For the purposes of this Policy, and in accordance with applicable law and the Privacy and Data Security Policy, the following terms shall have the following meanings:

a) **Data:** any information in the possession or control of the controller, whether public or confidential, for internal use, for restricted dissemination, or classified as a secret or personal data.

b) **Data file:** the set of data managed in a single register.

c) **Processing:** the totality of processing operations carried out by a Processor acting on behalf of or under the instructions of the Controller.

d) **Processor: a** natural or legal person or an unincorporated body which processes personal data on behalf of or under the instructions of the controller, within the limits and under the conditions laid down by law or by a legally binding act of the European Union.

e) **Processing:** any operation or set of operations which is performed upon personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

f) **Controller: a** natural or legal person, public authority, agency or any other body, including in particular in this case the Company, which alone or jointly with others determines the purposes and means of the processing of personal data, where the purposes and means of the processing are determined by Union or Member State law, the controller or the specific criteria for the designation of the controller may also be determined by Union or Member State law.

g) **Erasure:** rendering data unrecognisable in such a way that it is no longer possible to recover it.

h) **Data** breach**: a** breach of data security that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure or unauthorised access to, or unauthorised disclosure or access to, personal data transmitted, stored or otherwise processed.

i) **"Destruction" means the** case where the data do not exist at all or do not exist in a form that can be used by the Controller.

Examples:

- the data is accidentally or unlawfully (e.g. by an unauthorised person) deleted,
- the data storage medium is destroyed,
- paper documents containing the data are destroyed,
- rendering part or all of an IT system unusable by a virus or other malicious software.

➔ "Loss" of personal data: shall be understood to mean that the data still exist but the Controller no longer has control over, access to or possession of the data.

Examples:

- the data storage medium (laptop, thumb drive, company phone or even a paper folder) is lost,
- it will be stolen,
- the personal data are encrypted by the Controller but the key used for encryption is no longer in its possession,
- the password used to access the device is lost.

➔ "Modification, alteration": a case where the Controller processes the correct data, but for some reason during the processing the data is changed.

Examples:

- a part of the recorded video is cut out,
- the software used to manage the debt management fails and the amount of the debt is mixed up.

➔ Disclosing (or making available) personal data to unauthorised recipients:

Examples:

- sending documents or e-mail messages containing personal data to the wrong recipient,
- unlawful disclosure of personal data,
- making personal data available to unauthorised persons (e.g. sending e-mails to unknown recipients so that the recipients can learn each other's e-mail addresses)

The classification of an act as an incident does not depend on whether it was committed intentionally or unintentionally. So whether a data carrier is accidentally lost or stolen, it will be classified as a data breach.

j) **"De-identification" means the** processing of personal data in such a way that it is no longer possible to identify the natural person to whom the personal data relate without further information, provided that such further information is kept separately and technical and organisational measures are taken to ensure that no natural person who is identified or identifiable can be linked to that personal data.

k) **Biometric data:** any personal data relating to the physical, physiological or behavioural characteristics of a natural person obtained by means of specific technical procedures which allow or confirm the unique identification of a natural person, such as facial image or dactyloscopic data.

l) **Personal data relating to criminal matters:** personal data relating to the criminal offence or criminal proceedings, obtained during or prior to criminal proceedings, by the authorities competent to prosecute or investigate criminal offences, by the law enforcement authorities, which can be linked to the data subject, and personal data relating to the criminal record.

m) **Recipient: a** natural or legal person, public authority, agency or any other body to whom or with which personal data are disclosed, whether or not a third party. Public authorities which may have access to personal data in the framework of an individual investigation in accordance with Union or Member State law are not recipients, the processing of those data by those public authorities must comply with the applicable data protection rules in accordance with the purposes of the processing.

n) **Health data:** personal data relating to the physical or mental health of a natural person, including data relating to health services provided to a natural person which contain information about the health of the natural person.

o) **EEA State: a** Member State of the European Union and another State party to the Agreement on the European Economic Area, and a State whose nationals enjoy the same status as nationals of a State party to the Agreement on the European Economic Area under an international treaty concluded between the European Union and its Member States and a State not party to the Agreement on the European Economic Area.

p) **Data subject:** any natural person who is identified or can be identified, directly or indirectly, on the basis of specific personal data.

q) **Data subject's consent: a** voluntary, specific, informed and unambiguous indication of the data subject's wishes by which he or she signifies, by a statement or by an act expressing his or her unambiguous consent, that he or she signifies his or her agreement to the processing of personal data concerning him or her.

r) Supervisory Authority: an independent public authority established by a Member State in accordance with Article 51 of the Regulation, in Hungary the NAIH (Data Protection Supervisory Authority),

- Postal address: 1363 Budapest, Pf.: 9.
- Address: 1055 Budapest, Falk Miksa utca 9-11
- Phone: +36 (1) 391-1400
- Fax: +36 (1) 391-1410
- E-mail: ugyfelszolgalat@naih.hu
- URL: http://naih.hu

s) **Genetic data:** any personal data relating to the inherited or acquired genetic characteristics of a natural person which contain specific information about the physiology or state of health of that person and which result primarily from the analysis of a biological sample taken from that natural person.

t) **Child:** who has not reached the age of eighteen (minor).

u) **Third party: a** natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor or the persons who, under the direct authority of the controller or processor, are authorised to process personal data.

v) **Joint controller: a** controller who, within the limits set by law or by a legally binding act of the European Union, determines the purposes and means of processing jointly with one or more other controllers, takes and implements or has implemented decisions on processing (including the means used) jointly with one or more other controllers and with the processor.

w) **Special categories of data:** personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership, genetic data and biometric data revealing the identity of natural persons, health data and personal data concerning the sex life or sexual orientation of natural persons. The processing of special categories of data is in principle prohibited by Article 9(1) of the GDPR.

Although there are exceptions to this prohibition, where sensitive data may lawfully be processed, the handling of a data breach involving this type of data requires particular care in order to ensure that the Controller minimises the adverse effects on the data subject. In general, where an incident involves sensitive data, it is difficult to imagine that it would not entail a high risk to the rights and freedoms of data subjects.

x) **Profiling:** any form of automated processing of personal data whereby personal data are used to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict characteristics associated with that person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

y) **Personal data:** any information relating to an identified or identifiable natural person ("data subject"), an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Personal data is therefore any information relating to a natural person which directly or indirectly identifies or identifies that individual.

Personal data are individual identification data (e.g. name, place of birth, date, but also ID card number, social security number, tax identification number), location data (e.g. GPS coordinate), but also, for example, the username associated with a user account.

In this context, it should be stressed that proof of identity and identification are not the same Definitions. Only in exceptional cases is it necessary to provide all four natural identifiers (name, place of birth, date of birth, mother's name) for identification purposes; in most cases, the name and one of the three other identifiers is sufficient, provided that it is actually necessary for the identification of the data subject.

The quality of the personal data of e-mail addresses, especially "company" e-mail addresses, is a frequent issue. E-mail addresses of the type info@vállalkozás.com/iroda@company.com are not in themselves personal data, but e-mail addresses of the type vezetéknév.utónév@vállalkozás.com are, since they are in themselves capable of identifying the person concerned and are therefore personal data.

Personal data also includes any information (e.g. height, weight, hair colour, eye colour, language spoken, or any other characteristic) which, when combined, can identify a natural person (e.g. where it is possible to infer from a group of data who these characteristics refer to).

z) **Objection: a** statement by the data subject objecting to the processing of his or her personal data and requesting the cessation of the processing or the erasure of the processed data.

II. GENERAL RULES

II.1. Principles of personal data processing and the tasks to be carried out to ensure compliance with them

12. The Company respects the following principles in its data processing activities - for all data relating to data subjects:

i. Lawful, fair and transparent processing

13.The controller must process personal data in a fair and lawful manner and in a transparent manner for the data subject, including transparency about how their personal data is collected, processed, used and accessed. In order to implement the principle of transparency, the Controller shall endeavour to ensure that its information and communications relating to the processing of personal data are easily accessible and understandable and are drafted in clear and plain language.

14. The Controller shall inform the data subject of the essential characteristics of the processing in order to ensure the principle of transparency. The characteristics of the processing shall also be recorded in writing.

15. The Controller shall process the data in accordance with the data protection and sectoral legislation governing data processing.

16. The Controller shall inform the data subject of the essential characteristics of the processing in order to ensure the principle of transparency. The characteristics of the processing shall also be recorded in writing.

17.In accordance with the principle of lawfulness, the Controller shall continuously examine in all its processing whether the data have been processed in accordance with the applicable data protection legislation, in particular the GDPR and, where applicable, the Infotv., and whether the appropriate legal basis for the processing exists, and whether the data are processed on the basis of the appropriate legal basis.

18. For each processing operation, the Controller shall establish the legal basis for the processing and whether the necessary documentation supporting the legal basis for the processing is available. In particular, the legal basis for the Controller's processing and the necessary documentation:

(a) For processing based on the data subject's consent, a documented statement by the data subject or his or her legal representative giving his or her unambiguous consent to the processing of personal data concerning him or her, either in full or in relation to specific operations;
b) With regard to processing necessary for the performance of a contract concluded or to be concluded with the data subject, the contract concluded with the data subject;
(c) With regard to processing necessary for compliance with a legal obligation to which the controller is subject, the precise legal provision imposing or necessitating the processing;
(d) To carry out the balancing of interests test where the legitimate interests of the controller or a third party are asserted.

19. In order to document the processing based on consent, the Controller shall, for each processing based on consent, verify that:

a) Whether the documentation supporting the legal basis is available and has been obtained in accordance with the internal procedures;
b) Whether consent was the appropriate legal basis for the processing of the data;
c) The consent has been obtained in the correct format;
d) whether the data subject was duly informed before consent was given.

20.The Controller shall take technical and organisational measures appropriate to all the circumstances of processing, in particular its purpose and the risks to the fundamental rights of data subjects posed by processing, in order to ensure the lawfulness of processing. These measures shall be regularly reviewed and, where necessary, amended accordingly by the Controller.

21. The technical and organisational measures shall be designed by the Controller so that they:

a) are reasonably achievable, taking into account the state of the art and the cost of implementing the measures, to ensure the effective exercise of the requirements for the processing of personal data, in particular the principles of data processing and the rights of data subjects; and
b) suitable and adequate to ensure that, by default, personal data are processed only to the extent and for the duration necessary for the purposes for which they are processed and that personal data processed by the Company are not disclosed to the public in the absence of the data subject's explicit consent.

ii. Purpose limitation of data processing

22. Personal data may only be processed for specified, explicit and legitimate purposes and on one of the legal bases set out in the Regulation.

23. The Controller shall process personal data processed for a specific purpose for purposes other than the originally specified purpose only if there is an appropriate legal basis. The Controller shall duly inform the data subject of the processing for a purpose other than the original purpose before further processing.

24. The Controller shall ensure that personal data may be accessed only by its employees or processors whose processing is subject to the purpose limitation principle.

25. The Managing Director is responsible for ensuring the implementation of the purpose limitation principle in the organisation of the Controller.

26. At the start of the processing, the Controller shall specify the purpose of the processing. Once the purpose has been achieved, the personal data processed shall be deleted. The Controller shall not erase the data if the processing is also carried out for other purposes in the interest of the Controller or if the storage of the data is necessary for the exercise of the rights of the data subjects.

iii. Data economy

The Controller shall process only personal data that are adequate and relevant for the purposes for which they are processed and limited to the minimum necessary for that purpose, bearing in mind that personal data shall be processed only if the purposes of the processing cannot be achieved by any other reasonable means.

28. The scope of personal data necessary for the achievement of the specific processing purposes and the time of their processing, as well as the characteristics of each processing operation, are set out in the privacy notices published by the Controller.

iv. Accuracy

29. The personal data processed by the Controller are accurate and up to date. The Controller shall take all reasonable steps to ensure that personal data which are inaccurate for the purposes of the processing are erased or rectified without undue delay.

30. The Controller shall periodically review the accuracy and timeliness of the data maintained in its records in order to fulfil its obligation of accuracy.

31. The Controller shall in all cases draw the attention of the data subject to the fact that he or she shall notify any change to his or her personal data without delay.

v. Limited shelf life

32. Personal data are stored in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

33.The processing (storage) of data for a longer period than described in point 32 is only carried out for archiving purposes in the public interest, or for scientific and historical research or statistical purposes, or where necessary to ensure the exercise of the rights of data subjects.

34.The Controller shall determine the duration of the processing for each processing purpose, to the extent necessary to achieve the purpose, taking into account the applicable legislation, and shall also carry out the processing subject to the implementation of appropriate technical and organisational measures required to protect the rights and freedoms of the data subjects.

vi. Accountability

35. The Controller is responsible for compliance with the aforementioned principles and applicable law in the processing of personal data and must subsequently be able to demonstrate such compliance.

36. The Controller shall record in writing all relevant circumstances and actions taken in relation to the lawful processing of personal data, in particular, but not limited to, impact assessments carried out, interest assessments, the legal justification for decisions regarding processing and the fact of the data subject's consent, in order to comply with the principle of accountability.

37.The Company shall be liable for any damage caused by the unlawful processing of personal data or breach of data security requirements, the infringement of the personal rights of the data subject and shall be liable to compensate for such damage (damages and/or damages), if the infringement is finally adjudicated. The Company shall also be liable for any damage caused by a Processor it has engaged, unless the Processor has failed to comply with its obligations under the contract or the law or has disregarded or acted contrary to lawful instructions from the Controller. Liability for damage caused by a controller in a joint controller relationship with the Company shall also be borne by the Company, and the allocation of liability for damage between the Company and the joint controller may be determined by the contract concluded between them in their internal relationship.

vii. The principles of integrity and confidentiality

38.The processing of personal data shall be carried out in such a way as to ensure adequate security of personal data, including protection against unauthorised or unlawful processing, accidental loss, destruction or damage, in particular by preventing unauthorised access to or

use of personal data and the means used to process personal data, by implementing appropriate technical or organisational measures.

II.2. Data security

39. The Controller shall ensure the highest level of security of the personal data processed at all times during the processing (i.e. both in respect of data files stored by means of information technology and in respect of data files stored on traditional paper storage media). In doing so, it shall take the technical and organisational measures and establish the procedural rules necessary to enforce the Regulation and other personal data protection rules.

The Controller shall carry out its processing operations in such a way as to ensure adequate security of personal data and protection against unauthorised or unlawful processing, accidental loss, destruction or damage to data, by applying appropriate technical and organisational measures. In addition, the Controller shall take appropriate measures to protect personal data against, in particular, unauthorised access, alteration, disclosure, transmission, disclosure, erasure or destruction, accidental destruction or accidental damage and inaccessibility resulting from changes in the technology used. The Controller shall take the necessary technical and organisational measures to ensure this, taking into account the state of the art and the cost of implementation, the nature, scope, context and purposes of the processing and the varying degrees of probability and severity of the risk to the rights and freedoms of natural persons, both in respect of data files stored by means of information technology and in respect of data files stored on traditional paper storage media.

These measures may include in particular:

a) the pseudonymisation and encryption of personal data,
b) the continued confidentiality, integrity, availability and resilience of the systems and services used to process personal data,
c) in the event of a physical or technical incident, the ability to restore access to and availability of personal data in a timely manner;
can be set,
d) a procedure for the regular testing, evaluation and assessment of the effectiveness of the technical and organisational measures taken to ensure the security of processing.

41.In determining the measure to be implemented, the Controller shall, when determining the appropriate level of security, explicitly take into account the risks arising from the processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed.

42.The Controller shall design and implement its processing operations in such a way as to ensure the protection of the privacy of data subjects in the application of the law applicable to processing.

43.The Controller shall take the necessary measures to ensure that natural persons acting under its authority who have access to personal data may process the data in accordance with the purpose limitation principle only in accordance with its instructions, unless they are required to do otherwise by Union or Member State law.

The Controller shall take the necessary measures to ensure that access to the data is limited to the purpose for which it is intended and only to those persons who need to have access to the data in order to perform their tasks.

45. The Controller shall ensure the enforcement of data security rules by means of specific regulations, instructions and procedures. In order to enforce the conditions of data security, it shall ensure that the staff concerned are adequately trained.

46. The Controller or the designated department (if no such department is designated within the Company, the CEO) shall verify that the processed data are transferred to a controller or processor that ensures the security of the data.

47. When processing personal data, the Controller shall ensure that:

a) denying access to the means used for data management (the data management system) by unauthorised persons;
b) preventing the unauthorised input of personal data into the processing system and the unauthorised access to, modification or deletion of personal data stored in the processing system;
c) preventing the use of data processing systems by unauthorised persons by means of data communication equipment;
d) that persons authorised to use the system have access only to the personal data specified in the access authorisation;
e) that it is possible to verify and establish to which recipients the personal data have been or may be transmitted or made available by means of a data transmission installation;
f) to be able to verify and establish a posteriori which personal data have been entered into the system by whom, at what time;
g) preventing the unauthorised disclosure, copying, modification or deletion of personal data during transmission or transport of the data medium;
h) that the data management system can be restored in the event of a malfunction; and;
i) that the data management system is operational, that any errors in its operation are reported and that the personal data stored cannot be altered by the system's malfunction.

48. In order to ensure the security of personal data processed on paper, the Controller applies the following measures:

a) Measures to ensure protection against unauthorised access: o Data is only accessible to authorised persons and cannot be accessed or disclosed to others;
- access to active, ongoing files under management is only granted to the competent authorities;

b) Physical protection of documents: o Ensuring that documents are kept in a lockable room with security and fire alarm equipment;
- the Controller leaves the premises where data processing is taking place during the day only by locking the data media entrusted to him or by closing the office;
- the employee who is processing the data locks away the paper medium he or she has used after the end of the work

c) where personal data processed on paper are digitised, apply the security rules applicable to digitally stored documents;
d) paper documents containing personal data are destroyed in such a way that their content cannot be retrieved by any means (shredding);
e) in the absence of internal relevant rules of the Company, the notices issued in connection with each processing activity predetermine the storage period and the time of destruction of paper documents, which are based on a legal provision or a decision taken by the Controller in accordance with the provisions of the GDPR.

49. To ensure the security of personal data stored on the computer or network, the Controller applies the following measures and safeguards:

a) Measures to protect against unauthorised access:
- in the course of processing, employees primarily use tools that are the property of the Controller or over which the Controller has rights equivalent to ownership;
- access to the Controller's IT system from outside is possible securely, using only a username and password;

- access to the data on the computer is only possible with a valid, personal, identifiable authorisation - at least with a user name and password - and the Controller regularly ensures that passwords are changed;
- if the purpose of the processing has been achieved and the time limit for processing has expired, the data will be irretrievably deleted;
- employees are entitled to use only the e-mail address provided by the Controller in connection with their work (employees may not use this address for private purposes);

b) measures to ensure that the data files can be restored:

- regular backups;
- separate, secure management of copies (mirroring)

c) the Controller shall ensure virus protection and firewall protection on the network processing the personal data at all times;
d) the physical protection of data files and the media on which they are stored, including protection against fire, water, lightning and other natural hazards, and the recoverability of damage caused by such events (archiving, fire protection).

50. The Controller shall take special care to ensure the principle of data security in data transfers and shall only transfer data through secure channels.

51. If a restore from backup is carried out, the Controller shall ensure that deleted or corrected personal data cannot be restored.

52. The Controller shall print out electronically processed personal data only where this is expressly necessary for the exercise of a right or the performance of an obligation.

53. The Controller shall implement appropriate technical and organisational measures to ensure that, by default, only personal data that are necessary for the specific purpose of the processing are processed. This obligation relates to the amount of personal data collected, the extent to which they are processed, the duration of their storage and their availability. These measures ensure that personal data are by default not made available to an indeterminate number of persons without the intervention of a natural person.

54. The Controller shall ensure that access to the different categories of personal data is limited to employees in jobs whose job function relates to the processing of the personal data concerned. Employees shall have their own password and user account for computer systems, thus ensuring that unauthorised access is prevented. Paper files containing personal data are stored in such a way that only those employees who are authorised to handle personal data have access to them.

55. In order to protect the data files managed electronically in the different registers, the Controller shall ensure by appropriate technical means that the data stored in the registers cannot be directly linked and attributed to the data subject, unless permitted by law.

II.3. The person concerned

This Policy applies to the processing of personal data of any natural person.

57. Data subjects can be divided into several categories, in particular:

a) persons participating in events organised by the Controller (exhibitors, promoters, volunteers, visitors, press representatives covering the event);
b) interested;
c) natural person representatives, proxies, owners, contact persons of non-natural persons;
d) a person seeking to establish an employment relationship;
e) employee;
f) a relative of the employee.

58. The Company restricts the processing of children's data to the processing of employees' children's data that is necessary in connection with family tax allowance and child tax credit.

II.4. Processing of the data of the deceased

59. Within 5 (five) years of the death of the person concerned, the deceased shall be entitled to:

a) the right of access to;
b) the right to rectification;
c) the right to restriction of processing;
d) the right to erasure and the right to object;

by a person authorised by the data subject by means of an administrative order or a declaration in a public or private document having full probative value made to the Company as controller or, if the data subject has made more than one declaration, by a declaration made at a later date.

60. If the data subject has not made a declaration of rights under the previous point, his or her close relative within the meaning of the Civil Code is entitled to do so even in the absence of such a declaration:

a) the right to rectification and opposition, and
b) (where the processing was unlawful during the lifetime of the data subject or the purpose of the processing ceased to exist upon the death of the data subject) the right to restriction of processing and the right to erasure, enforce the rights of the deceased during his or her lifetime within 5 (five) years of the death of the person concerned. The right to enforce the rights of the person concerned under this point shall be exercised by the next of kin who first exercises that right.

61. The person who asserts the rights of the data subject under the above shall provide proof of the fact and date of death of the data subject by means of a death certificate or a court order, and shall provide proof of his or her identity and, where applicable, of his or her status as a close relative, by means of a public document.

62.The Company as controller shall, upon request, inform the close relative of the data subject within the meaning of the Civil Code of the measures taken pursuant to the above, unless the data subject has prohibited this in a statement made to the Company as controller.

II.5. Purpose of data processing

63. Personal data may only be processed for specified and unambiguous purposes, and the purposes for which the processing is to be carried out must be clearly specified prior to the processing.

64. If the purpose of the processing cannot be determined, the processing shall not take place.

65. The purposes of the processing of personal data covered by this Policy may include, in particular:

a) identification of the person concerned (partner, employee, etc.), ensuring contact;
b) the conclusion of a contract;
c) performance of a contract;
d) payment of the remuneration for the partner's activities;
e) records of litigation;
f) enforcement of claims;

g) providing information;
h) accreditation;
i) any other activities carried out by the Controller in the course of which personal data are processed.

66. The purpose of the processing must be fulfilled at all stages of the processing.

67. The Company processes personal data only for lawful purposes. In order to ensure this, once the purposes for which the processing is envisaged have been determined, it is necessary to verify that the purposes for which the processing is envisaged are legitimate in all respects. If the purpose of the processing is not lawful, the processing shall not take place.

II.6. Scope of personal data processed

68. Once the purpose of the processing has been specified, the data to be processed must be precisely and unambiguously determined.

69. Once the data have been identified, it is necessary to classify them, to determine whether or not the data are personal data. In particular, the following are considered personal data: name, name at birth, mother's name, address, postal address, place of birth, date of birth, nationality, identity card number (identity card, passport, driving licence), tax identification number, social security number, telephone number (landline, mobile), e-mail address (work, private), fax number, bank account number, signature.

70. If the data to be processed is not personal data, the provisions of this Policy do not apply to its processing.

71. If the data to be processed is personal data, it must be examined whether the data

a) whether it constitutes sensitive data;
b) whether it is personal data that the Company may process (taking into account that some personal data may not be processed by the Company or may be processed only exceptionally).

72. The processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership, as well as the processing of genetic data and biometric data revealing the identity of natural persons, health data and personal data concerning the sex life or sexual orientation of natural persons is prohibited. Such data shall also be erased without undue delay where they have been provided by the data subject without any prompting.

73. If the personal data to be processed cannot be processed by the Company, the processing shall not take place.

II.7. Legal basis for processing

74. The processing of personal data is lawful only if and to the extent that at least one of the following conditions is met:

a) the data subject has given his or her consent to the processing of his or her personal data for one or more specific purposes;
b) the processing is necessary for the performance of a contract to which the data subject is a party or for taking steps at the request of the data subject prior to entering into the contract;
c) processing is necessary for compliance with an obligation under Union or national law to which the controller is subject;

d) processing is necessary for the protection of the vital interests of the data subject or of another natural person;
e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where those interests are overridden by the interests or fundamental rights and freedoms of the data subject which require the protection of personal data, in particular where the data subject is a child (legitimate interest ground).

75.Where the Controller processes personal data for purposes other than the purpose for which the data were collected and the processing is not based on the data subject's consent or on a legal provision, the Controller shall take into account the following before starting the processing:

a) the purposes for which the personal data are collected and any links between the purposes for which further processing is envisaged;
b) the circumstances in which the personal data have been collected, in particular the relationship between the data subjects and the Controller;
c) the nature of the personal data, in particular whether special categories of personal data are processed and whether data relating to criminal liability and criminal offences are processed;
d) the possible consequences for the data subjects of the envisaged further processing of the data;
e) the existence of appropriate guarantees.

i. Consent as legal basis

76. Where processing is based on consent, it is lawful only if the Controller obtains consent in such a way that it is able to demonstrate later that the data subject has given his or her consent to the processing of his or her personal data and that his or her consent is given in good faith:

a) voluntary (giving the data subject a real or free choice and the possibility to refuse or withdraw consent without detriment);
b) based on specific and adequate information;
c) an unequivocal statement by the data subject, either by a declaration or by an act expressing his or her consent in an unequivocal manner his or her confirmation, that he or she gives his or her consent to the processing of personal data concerning him or her.

77. In order to comply with the above criterion, prior to processing based on the data subject's consent, the Controller shall inform the data subject of the relevant facts concerning the processing, as set out in the policies and procedures for complying with the data subject's request. The content of the information shall comply with legal requirements and its language shall be comprehensible, clear and simple for the data subject. In the absence of such information, the data subject's consent cannot be deemed to have been given, as he or she will not be able to take a meaningful decision regarding his or her data.

78. Consent may take the form of a written (including by electronic means) or oral] statement or an unambiguous act expressing consent, in particular by ticking a box when visiting a website, by making technical settings when using information society services, or by any other statement or act which, in the relevant context, unambiguously indicates the data subject's consent to the intended processing of his or her personal data. Silence, ticking a box or inaction does not constitute consent.

79. Consent covers all processing activities carried out for the same processing purpose or purposes.

80. The consent form, regardless of its form, must comply with the following conditions:

a) be clear;
b) can be separated from other cases;
c) clear, understandable, plain language.

81.In view of the above, where the data subject gives his or her consent in a written contract or other statement that also relates to other matters, the request for consent must be presented in a manner clearly distinguishable from those other matters, in a clear and easily accessible form, in clear and plain language.

82.Where the data subject gives his or her consent following an electronic request, the request must be clear and concise and must not unnecessarily impede the use of the service for which consent is sought.

83.The processing of data by an employer may be based on consent, exceptionally, only if the employee has the possibility to refuse consent due to the nature of the subordinate or superior relationship arising from the employment relationship.

84. The data subject has the right to withdraw his or her consent at any time. The Controller shall inform the data subject of this prior to giving consent and that the withdrawal of consent shall not affect the lawfulness of the processing based on consent prior to the withdrawal. The Controller shall make it as easy to withdraw consent as it is to give it.

85. The Company shall keep the declaration of consent to personal data processing for the duration of the processing.

ii. Use of a contractual legal basis

86. The Controller has an adequate legal basis for processing where processing is necessary for the performance of a contract to which the data subject is a party or for taking steps at the request of the data subject prior to entering into the contract.

This legal basis therefore applies:

a) in the case of direct actions for the conclusion of a contract (invitation to tender, submission of tenders, negotiation of contractual terms), if they are carried out at the request of the data subject; or
b) where the data subject is a party to a valid and effective contract and the processing is necessary for the performance of that contract.

87. The legal basis must be interpreted strictly, so that it can only be used if there is a direct and objective link between the processing and the performance of the contract. The legal basis also covers processing carried out before the conclusion of the contract, including pre-contractual relations, provided that it is not initiated by the Company or a third party but by the data subject.

88. This legal basis does not apply where the processing is not actually necessary for the performance of a contract, in particular where the processing is carried out in the context of the non-performance of a contract. Nor may data be processed on the basis of this legal basis where such data may also be processed on the basis of point 74(e).

iii. Fulfilling a legal obligation

89. The fulfilment of a legal obligation is the legal basis for processing where the processing is provided for by a law, a regulation of a local government or a binding legal act of the European Union which specifies the types of data to be processed, the purposes and conditions of the processing, the availability of the data, the identity of the controller and the

duration of the processing or the need for periodic review. In this case, the Controller shall inform the data subject by indicating the specific legal provision requiring the processing.

90. If a law or regulation imposes a legal obligation which the Controller can only fulfil by processing personal data, but the law does not specify the exact circumstances of the processing, i.e. in the case of this legal requirement, the provisions of the Infotv. 5(3) of the Regulation, the legal basis under Article 6(1)(c) of the Regulation does not apply. Also, this legal basis does not apply if the law provides for the possibility of processing, but does not oblige the controller to do so and the provisions of the Infotv. Article 5(3) is missing.

91. In this case, the legal basis for the processing is determined by EU or Member State law. Union or Member State law must serve a public interest purpose and be proportionate to the legitimate aim pursued. In this case, the Company has no discretion as to whether or not to fulfil the obligation.

92.Unless the duration or the periodic review of the necessity of the mandatory processing is determined by law, local government regulation or a binding legal act of the European Union, the Company as the controller shall review at least every 3 (three) years from the start of the processing whether the processing of personal data processed by it or by a Processor acting on its behalf or at its instructions is necessary for the purposes of the processing. The Company shall document the circumstances and the results of this review and shall keep this documentation for 10 (ten) years after the review has been carried out and shall make it available to the NAIH upon request.

93. The legal basis does not exist if the legal obligation is fixed by contract.

iv. Legitimate interest as a legal basis

94.Processing may be carried out in accordance with Article 74(f) of this Policy if the processing is necessary for the purposes of the legitimate interests pursued by the Controller or a third party, unless such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require the protection of personal data, in particular where the data subject is a child.

95. Before the processing starts, the Controller shall carry out an interest test to determine to what extent the legitimate interests of the Controller adversely affect the rights and freedoms of data subjects.

96. Where the legal basis for the processing envisaged by the Company is likely to be the legitimate interest of the Company, the balancing of interests shall be carried out by the Interest-Balancing Committee established for this purpose on a case-by-case basis, which shall be composed of at least:

a) the person designated by the head of the department within the Company (if the activity concerned by the processing is carried out by a separate department within the Company) or the employee who actually carries out the processing;
b) the administrator.

97. The head of the professional area in which the Company intends to carry out the processing (if the activity concerned by the processing is carried out by a separate department within the Company) or the employee who actually carries out the processing shall provide prior information on the intended processing to the Chief Executive, who shall decide on the establishment of the Interest-Balancing Committee. The body to be set up shall take its decisions by a majority of votes cast, and in the event of a tie, the Executive Director shall decide on the outcome of the balancing of interests. The member of staff who will actually carry out the planned processing shall participate in the work of the committee.

98. The balancing of interests must be carried out before the processing based on the Company's legitimate interests is started, in accordance with the legal requirements and this Policy, and approved by the CEO.

99. Processing based on the legitimate interests of the Company shall not be initiated if the balancing of interests has not been carried out.

100. The Interest Weighing Committee shall document in writing the conduct of the interest weighing and its results in detail, including all steps of the interest weighing. Detailed written documentation of the interest-testing is not required if the processing is permitted by law.

101.Processing based on the legitimate interest of the Company may only be started if the Interest Selection Committee, after conducting an interest selection, has determined that the legitimate interest of the Company constitutes a legal basis for the processing and that the interests of the Company prevail over the interests, fundamental rights and freedoms of the data subject.

102.If, after conducting the balancing of interests, the Balancing of Interests Committee is not in a clear position as to whether the legitimate interests of the Company constitute a legal basis for the processing, it may consider contacting the NAIH for a position.

103. In the test, the Controller:

a) examine whether the processing is necessary;
b) determine its own or a third party's legitimate interest;
c) identify the interests of the data subjects to be protected;
d) specify the measures and safeguards taken to protect the interests of the data subject
e) balance its own legitimate interests with those of the data subjects,
f) determine whether the processing can be lawfully carried out.

104. The following steps can be distinguished in the data protection interest assessment process:

Step 1: Determining the purpose of the processing
Step 2: Examination of the lawfulness of the purpose of the processing
Step 3: Identification and classification of the data to be managed
Step 4: Examination of the legal basis for processing
Step 5: Identify the obstacle to data processing
Step 6: Determining the Company's interest in data management
Step 7: Determining the legality of the Company's interest
Step 8: Examination of the necessity or unavoidability of the processing by the Company
Step 9: Assessing the Company's interest
Step 10: Assessing the impact of processing on data subjects
Step 11: provisional assessment
Step 12: Additional safeguards applied by the Company
Step 13: Final assessment
Step 14: Ensuring transparency
Step 15: Repeat the interest test

The data subject's right to the protection of personal data and his or her rights relating to privacy must not, unless an exception is provided by law, be affected or limited by other interests in the processing, including the disclosure of data of public interest.

II.8. Content of data processing

105.The data processing activities of the Company include operations on personal data and data files, in particular collection, recording, organisation, structuring, storage, transformation, alteration, consultation, access, use, disclosure by transmission, dissemination or otherwise making available, alignment, combination, restriction, erasure, destruction.

106. In the event of restriction of processing, the Company shall ensure that no further processing operations are performed on the personal data and that they cannot be altered. In particular, in the event of restriction of processing, the personal data in question may be:

a) temporary transfer to another data management system,
b) to remove their availability to users,
c) temporarily remove it from the website.

107. Real personal data may not be used to verify the correctness of computer and telecommunications equipment and programs, to train users or for educational purposes. In IT (functional, integration) test environments, it must be ensured that the link between personal data processed in the live system and the anonymised data used in the test environment cannot be technically restored. In IT test environments (functional, integration), the use of personal data without anonymisation is prohibited as a general rule. Exceptions to this rule may be made only if testing would be impracticable or infeasible without it. In this case, however, a risk acceptance statement is required from the head of the business area concerned or, failing this, from the managing director. Even then, however, the use of personal data should be kept to a minimum and, where possible, replaced by non-real data or masked, truncated or otherwise anonymised in some way, while ensuring that the link between the personal data processed in the live system and the (anonymous) data used in the test environment cannot be technically re-established, if possible.

II.9. Duration of data processing

108. Personal data may only be processed in a way that permits identification of the data subjects for the time necessary to achieve the purposes of the processing.

109. The Company shall keep the personal data at its disposal in accordance with the various processing purposes and legal bases, and where required by law, shall delete the data, or, where it has the possibility to do so, anonymise them, taking into account the interests of the data subject and the Company, in particular where it is clear that the data will no longer be used or the purpose of the processing has ceased.

110. The retention period may be in particular:

a) in the case of processing based on the consent of the data subject, the period until the withdrawal of the consent,
b) in the case of processing based on the legitimate interests of the Company, the period limited by the interest of the processing or the loss of the purpose of the processing or the successful objection of the data subject to the processing,
c) the period after the termination of the contractual relationship between the Company and the data subject until the end of the limitation period (unless otherwise provided by law),
d) in the case of compulsory processing based on law, the expiry of the time limit provided for in the relevant legislation, for example 5 (five) years in the context of taxation, and 8 (eight) years in the context of accounting.

111. In order to ensure that the storage of personal data is limited to the necessary period, the Company will set time limits for erasure or periodic review.

II.10. Termination of data processing, erasure and destruction of personal data

112.If the purpose of the processing carried out by the Company has been achieved, the Company no longer needs the processed data, the processing of the personal data concerned shall be discontinued, the data deleted or destroyed pursuant to a legal requirement or a decision of an authority or court or for any other reason.

113. The method of storing the data by computerised means shall be chosen in such a way that their deletion can be carried out at the expiry of the deadline for deletion or if otherwise necessary, also taking into account any different deletion deadline. The personal data must be erased in such a way that the data are rendered unrecognisable and irretrievable and that the erasure is irreversible and verifiable.

114. Paper data media shall be destroyed by shredding or by using an external contractor specialised in shredding. In the case of electronic data media (hard disks, optical media, magnetic media, printers, back-up disks of multifunctional machines, flash (NAND) media, SIM cards, mobile devices, telephones, PDAs, tablets, laptops, etc.), physical destruction and, if necessary, prior secure and irretrievable deletion of the data shall be ensured in accordance with the rules on the disposal of electronic data media. The destruction of data media shall be controlled, documented, retained in a retrievable form and disposed of in accordance with the provisions of the relevant policy. In relation to this Policy, the method of disposal of personal data contained in the Electronic Media shall be the complete deletion of the document containing the data or, if this is not possible under the legal provisions on records management or disposal, the rendering of the personal data unrecognisable in such a way that it can no longer be retrieved.

115. The obligation to erase data cannot be fulfilled by pseudonymisation alone, since the pseudonymised personal data can be subsequently linked to a natural person by using additional information and thus be considered as data relating to an identifiable natural person.

116. The physical deletion of data fulfils the obligation to delete data. Physical deletion of data is then performed, either by the actual deletion of the record or by the physical overwriting of the data to be deleted (e.g. by entering "X" characters in the appropriate field)

117. Logical deletion is acceptable if the solution effectively results in ensuring the non-recognition of personal data and preventing re-use.

118. A method of deletion that cannot even be considered as a logical deletion, where the deleted data are faintly but clearly legibly displayed on the interface and the data are still present in the IT system, still in a visible, recognisable form in the database, is not acceptable - this deletion technique does not terminate the processing.

II.11. Processing of special categories of personal data

119.The processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership, as well as genetic data and biometric data for the purpose of uniquely identifying natural persons, health data and personal data concerning the sex life or sexual orientation of natural persons, is lawful only if at least one of the following conditions is met:

a) the data subject has given his or her explicit consent to the processing of those personal data for one or more specific purposes;
b) processing is necessary for the purposes of complying with the obligations and exercising the specific rights of the controller or of the data subject arising from legal provisions governing employment, social security and social protection;
c) the processing is necessary for the protection of the vital interests of the data subject or of another natural person where the data subject is physically or legally incapacitated and is unable to give his or her consent;
d) the processing relates to personal data which have been explicitly made public by the data subject;

e) processing is necessary for the establishment, exercise or defence of legal claims or where the processing is necessary for the exercise of judicial or quasi-judicial functions.
are acting within their remit;
f) the processing is necessary for an important public interest, on the basis of Union or national law, is proportionate to the aim pursued, respects the essential content of the right to the protection of personal data and provides for adequate and specific measures to safeguard the fundamental rights and interests of the data subject;
g) processing necessary for preventive health or occupational health purposes, to assess the ability of an employee to perform his or her job, to make a medical diagnosis, to provide health or social care or treatment, or to manage health or social systems and services, under Union or Member State law;
h) the processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes on the basis of Union or national law which is proportionate to the aim pursued, respects the essential content of the right to the protection of personal data and provides for adequate and specific measures to safeguard the fundamental rights and interests of the data subject.

II.12. Ensuring the rights of the data subject

120.The Company shall ensure the exercise of the following rights of the data subjects in relation to the processing of their personal data by the Company, cooperating with the data subjects in the exercise of those rights.

a) right to information (about the recipients informed about the processing, rectification, erasure and restriction of processing of personal data);
b) right of access;
c) the right to rectification;
d) the right to erasure;
e) the right to be forgotten;
f) the right to restriction;
g) the right to data portability;
h) the right to object;
i) the right to a remedy.

121. The Company shall take appropriate technical and organisational measures to facilitate the exercise of the rights of the data subject, in particular:

a) endeavour to provide any notifications and information to be given to the data subject in an easily accessible and legible form, in a concise, clear and plain language; and
b) examine the request for the exercise of the rights to which the data subject is entitled, within the shortest time limit provided for by law and as soon as possible after the request is made, and notify its decision to the data subject in writing or, if the request was made by electronic means, by electronic means.

122. If the data subject approaches the Company in connection with the exercise of his/her rights, the provisions of the Rules on the Procedure for the Enforcement of Data Subjects' Rights in force at the Company shall apply.

III. PARTIES TO THE PROCESSING

III.1. Organisation of data management

123. The following are involved in the management and performance of data protection activities:

a) the managing director

i. The Managing Director

124. The Controller shall be headed by the Executive Director. The administrator shall be responsible for the data protection activities of the Controller:

a) is responsible for the lawfulness of the Controller's processing;
b) define and establish internal rules, internal systems of rules and procedures for data protection, taking into account the specificities of the Controller;
c) is responsible for ensuring the conditions necessary for the exercise of the rights of data subjects under the law;
d) is responsible for ensuring the personal, material and technical conditions necessary for the protection of the personal data processed by the Controller;
e) be responsible for complying with the requests of the data subject;
f) represent the Controller in relation to requests from external bodies and persons concerning the processing of personal data by the Controller;
g) be responsible for remedying any deficiencies or unlawful circumstances found during the control of data processing, and for initiating or conducting any proceedings necessary to establish personal liability;
h) ensure that the Controller only uses the services of Processors that process personal data in compliance with the applicable legislation;
i) establish the responsibilities and powers for data protection and related activities and designate the authorities for the processing of personal data and monitor compliance with those responsibilities and powers;
j) direct and instruct the heads of the departments of the Controller (if the work is divided into departments within the Company) or its employees as regards data processing;
k) organise the work of the organisational units (if the work is divided into organisational units within the Company) or subcontractors of the Controller in such a way that only those employees participate in the processing of personal data who need to do so for the performance of their tasks, and that personal data cannot be accessed, learned, altered or destroyed by unauthorised persons;
l) provide data protection training for employees;
m) be responsible for the compliance with the time limits for the deletion of data and for the deletion of data when the time limits have expired;
n) is responsible for the accuracy and updating of records.

ii. Heads of departments

(where the work is not carried out within the Company on a departmental basis, the provisions set out in this Part of the Code shall apply to employees carrying out data processing activities, subject to the necessary derogations)

125. The heads of specific departments of the Controller are responsible for the lawfulness of the processing of personal data by the departments under their control. The head of a given department shall, taking into account the specificities of the data processing activities, determine the organisation of data protection in that department, the tasks and responsibilities for data protection and related activities on the basis of instructions from the administrator.

126. Heads of department - in respect of the department under their authority
- on data protection:

a) order a personal data processing investigation;
b) shall forward the requests of the parties concerned to the administrator and cooperate in their execution;
c) forward to the Executive Director requests received from external bodies and persons;
d) provide the person(s) designated to keep the records with all the information necessary for the proper keeping of the records under this Policy in a timely manner (they shall be fully responsible for the completeness, accuracy and timeliness of the information provided);
e) under the instructions of the administrator, be responsible for remedying any deficiencies or unlawful circumstances which may be discovered during the control of data management, and for initiating or conducting any proceedings necessary to establish personal liability.

127. The administrator shall assist in the implementation of his/her decision pursuant to point 124(l) and organise the work of the department under his/her control in such a way that personal data are processed only by those employees who need to know them for the performance of their duties and that personal data are not accessible, known, altered or destroyed by unauthorised persons.

iii. The employee involved in the processing

128. In the course of performing his or her duties, the employee shall ensure that no unauthorised person has access to the personal data processed by him or her in the course of performing his or her duties, and shall ensure that the personal data are stored and stored in such a way that they cannot be accessed, accessed, altered or destroyed by unauthorised persons.

129.The employee is responsible for the processing, modification, deletion, transmission and disclosure of data within the scope of his or her duties, as well as for the accurate and traceable documentation of data, and for keeping and updating records. In the course of his/her activities, he/she shall, where necessary, consult with the head of the department (if the work is carried out within the Company on a departmental basis) or the Managing Director prior to the data processing operation.

130. Employees shall handle and retain the data obtained in the course of their duties or work, and shall be entitled to transmit such data only on the basis of the law or on the instructions of the head of the department (if the work is divided into departments within the Company) or the Managing Director, in full compliance with the provisions of this Policy.

131.The employee shall also be obliged to keep business secrets disclosed to him/her in the course of his/her work in accordance with Article 8 (4) of Act I of 2012 on the Labour Code. In addition, he shall not disclose to any unauthorised person any information which he has acquired in the course of his employment and the disclosure of which could have a detrimental effect on the Controller or any other person. Confidentiality shall not extend to the statutory obligations to provide information and to disclose data of public interest and to provide information on data of public interest.

132.The employee shall immediately report any irregularities in data management to the head of the department (if the work is divided into departments within the Company) or to the managing director and, if necessary, participate in their elimination.

133. In the course of his/her activities, the employee shall comply with the legislation on data management and the provisions of this Code.

134. The employee shall process the personal data on the technical means and with the software designated by the Controller. Other hardware and software may be used only with the prior written consent of the Administrator.

135. The employee is entitled to transmit data containing personal data only through a secure channel. If in doubt as to the adequacy of the security of the communication channel to be used, the employee must seek the instructions of the head of the department (if the work is split into departments within the Company) or the managing director before transmitting the data.

136. The employee uses password protection for all devices used to manage personal or business data.

137. Whenever possible, data matching should be carried out when communicating with the data subject, provided that the communication channel is sufficiently secure.

138. The employee shall participate in data protection training organised by the Controller.

The employee shall inform the head of the department (if the work is divided into departments within the Company) or the managing director of any event in which he/she has been requested or instructed to carry out unlawful processing or has experienced any other unauthorised access to or processing of data on his/her own system.

III.2. Shared data management

140. Where a controller determines the purposes and means of processing for which it is responsible jointly with another controller (hereinafter jointly referred to as "joint controllers"), it shall be considered joint processing. Joint controllers shall, before joint processing commences, conclude an agreement in which they shall set out in a transparent manner the division of their responsibilities for fulfilling the obligations imposed on them by data protection law, in particular their duties in relation to exercising the rights of the data subject and informing him or her of the processing, unless the division of responsibilities is provided for by law.

141. The agreement shall designate a contact person for the data subjects, if necessary.

142. The substance of the agreement shall be made available to the data subjects, as specified in the agreement between the joint controllers.

143. The data subject may exercise his or her rights under the law in relation to and against each controller irrespective of the terms of the agreement. The joint controllers shall cooperate in relation to the provision of those rights.

144. The agreement between the Company and the other controller shall, subject to the above, specify in particular:

a) the purpose of the processing;
b) the scope of the data to be processed;
c) the duration of the processing;
d) the processing operations to be carried out by each controller involved in joint processing (recording of consent statements, storage of recorded data);
e) the tasks of each controller in providing information to data subjects on data management;
f) the tasks of each controller in the enforcement of the rights of data subjects and the rules for bearing the consequences of any unlawful processing;
g) the applicable data security measures;
h) the procedure to be followed in the event of a threat or occurrence of a personal data breach;

i) the rules on the designation of a contact point which may be designated for the data subject, the identity of the contact point, its contact details and the rules on the modification of the contact point;
j) a summary of the agreement between the joint controllers to be made available to data subjects.

III.3. The Processor

145. If a natural or legal person carries out any data processing operation in the course of its activities on behalf of and on behalf of another person, the person acting on behalf of another person shall be considered a Processor within the meaning of Article 4(8) of the Regulation in respect of such operation(s) and the data transferred, and shall carry out data processing pursuant to Article 3(17) of the Data Protection Act.

i. Mandate of a Processor by the Controller

The Controller shall conclude a data processing contract with a natural or legal person who processes personal data on behalf of the Controller on the basis of a mandate and instructions from the Controller, with the content of Article 28 of the Regulation. The Processor shall act only on the basis of written instructions from the Controller and shall not take any substantive decision regarding the processing. If the Processor goes beyond the scope of the mandate, in particular if it processes data for purposes other than those for which it was mandated (including its own), it becomes an independent controller in respect of that overlap.

147. The data processing contract shall clarify at least the following issues:

a. the processing purposes for which the Controller uses the services of the Processor;
b. the Controller activity performed by the Processor;
c. the duration, nature and purpose of the processing;
d. the type of data transferred for processing;
e. the categories of data subjects concerned by the processing;
f. the rights and obligations of the Controller;
g. the rights and obligations of the Processor.

148. The Controller shall only enter into a contract with a Processor for a data processing task where the Processor undertakes in the contract to:

a. Process personal data only on the basis of the Controller's written instructions, including the transfer of personal data to a third country or international organisation, unless the processing is required by Union or Member State law applicable to the Processor, in which case the Processor shall notify the Company of that legal requirement prior to processing, unless the Company is prohibited from doing so by the relevant legislation on grounds of important public interest. The Processor shall inform the Company without undue delay if it considers that any of its instructions is in breach of national or EU data protection provisions.

b. Ensure that the persons involved in the processing of personal data are bound by an obligation of confidentiality or are under an appropriate obligation of confidentiality based on law.

c. It shall take the data security measures required by Article 32 of the Regulation, such as implementing appropriate technical and organisational measures to ensure a level of data security appropriate to the scale of the risk, with varying degrees of probability and severity, to the rights and freedoms of natural persons.

d. The Controller shall not use any other Processor without prior written authorisation, either ad hoc or general.

e. To the extent possible, and taking into account the nature of the processing, assist the Controller in fulfilling its obligation to respond to requests relating to the exercise of the rights of data subjects, by appropriate technical and organisational measures.

f. Assist the Company in fulfilling its other obligations in relation to data processing, taking into account the nature of the processing and the information available to the Processor.

g. In the event of a data breach, notify the Controller without delay as soon as the Controller becomes aware of the data breach and cooperate in the handling of the data breach;

h. Upon completion of the provision of the processing service, the Controller shall, at the Controller's discretion, delete or return to the Controller all personal data and copies of personal data at the same time.
destroy or delete it;

i. Enable and facilitate the Controller or other auditor appointed by the Controller to verify (through audits or on-site inspections) the implementation of the data protection rules.

j. Maintain the register of Processors pursuant to Article 30(2) of the Regulation.

149. In addition to the provisions of Clauses 147 and 148, the data processing contract between the Company and the Processor shall also provide for:

a. the Processor shall notify the Company without undue delay if any of the data subject:
- has contacted you to exercise his or her rights of access, rectification, erasure, restriction of processing or portability,
- lodges a complaint alleging a breach of the legal provisions on data processing,

b. the Processor shall notify the Company without undue delay if it has received a request from a data protection supervisory authority (NAIH) or any other authority or court concerning the Company's data processing activities;
c. the Processor shall cooperate with the Company in order to respond to requests from the data subject or from public authorities or courts;
d. the Processor shall assist the Company in fulfilling the Company's obligations in relation to the security of data processing, the notification of a data protection incident to the data protection supervisory authority (https://www.naih.hu/adatvedelmi-incidensbejelent--rendszer.html), the data protection impact assessment and prior consultation, taking into account the nature of the processing and the information available to the Processor,
e. in the context of the assistance, the Processor shall, in particular, as instructed by the Company:
- inform the data subject about the processing of personal data,
- provide the data subject with a copy of the personal data in the possession of the Processor which are the subject of the processing,
- correct or delete the personal data.

150. The contract for data processing must be in writing.

151. Before the processing starts, the Controller shall ensure that the Processor has taken the necessary technical and organisational measures to ensure an adequate level of data protection in its day-to-day activities.

152. The rights and obligations of the Processor in relation to the processing of personal data shall be determined by the administrator. The administrator or the person designated by him shall have the right to instruct the Processor on behalf of the Controller. The employee who

has been given the right to give instructions shall be responsible for the lawfulness of the instructions given by him or her.

153. The processing must not be entrusted to an entity that is engaged in a business activity involving the use of personal data.

154. The Processor shall not engage any other Processor without the prior written authorisation, whether general or ad hoc, of the Company. In the case of a general written authorisation, the Processor shall inform the Company of any planned changes affecting the use of additional Processors or their replacement, thereby giving the Company the opportunity to object to such changes.

155. The Company may withdraw any approval to use a specific additional Processor (subcontractor). The Company shall, at the time of revocation, inform the Processor of the reasons for the revocation.

ii. Processing activities carried out by the Controller

156. If the Controller carries out any data processing activity on behalf of another (legal) person on the basis of the latter's mandate, the Controller shall be considered a Processor pursuant to Article 4(8) of the Regulation in respect of the mandated operation(s), and shall carry out data processing pursuant to Article 3(17) of the Data Protection Act.

157. With regard to the fact of processing, the Controller shall conclude a data processing contract with the Principal as referred to in point III.3.i. of these Rules.

158. The controller is entitled and obliged to give written instructions to the controller in relation to the processing. The principal shall be responsible for the lawfulness of the instruction. The Controller may only carry out its processing activities on the basis of such an instruction and may not take any substantive decisions concerning the processing, nor may the Controller determine the purposes for which the data are processed or use the data for any other purposes.

III.4. Data transmission

159. The Company shall endeavour to limit the transfer of data, the amount of data transferred, the possible purposes for which it may be processed and used, the possible duration of its processing and the possible recipients of its transfer.

160.The Company shall, at the same time as the transfer, declare to the data recipient whether the data recipient will process the personal data received and relating to the data subject to the extent and in a manner consistent with the applicable data processing restriction, and whether the data subject's rights will be safeguarded in accordance with the data processing restriction, and shall request an undertaking that, if this becomes important for the Company for any reason, the data recipient will also separately inform the Company about the processing and use of the personal data received.

i. Transfers to an EEA State

161. Transfers to an EEA State shall be deemed to have taken place on the territory of Hungary.

162. A transfer is the making available of personal data to a specified third party. A third party is any person or organisation other than the Controller, the data subject and any processor that is an independent controller and does not fulfil the conditions for joint processing.

163.The Controller shall verify, prior to the transfer of the personal data it is processing, whether the conditions for the transfer of the personal data are met, in particular whether it is

a controller of the data requested, whether it has a legal basis for the transfer and whether the transfer complies with the purpose limitation principle.

164. It is the responsibility of the employee carrying out the transfer to check that the conditions for the transfer are met. The transfer of data for processing does not constitute a transfer within the meaning of the above.

165. Except in the case of a mandatory transfer, the administrator shall be responsible for the processing of a request for transfer submitted by a third person or body. A request for transfer may be granted if it contains:

a) the data necessary to identify the data subject beyond reasonable doubt;
b) the purpose of the transfer, the legal basis for the transfer (specifying the legal provision on which the transfer is based);
c) a precise definition of the scope of the data requested;
d) the data necessary to identify the person concerned.

166. The Controller shall keep a record of its transfers, the rules for keeping which are set out in Chapter V of these Rules.

167. If the transfer cannot be lawfully carried out or the information necessary for the assessment of the claim has not been provided by the claimant after the request, the transfer shall be refused. The refusal to transfer shall be notified in writing to the claimant, together with the reasons for the refusal.

168. The transfer of data may be made on the basis of a request by individual data supply or, by law or by agreement, by direct access.

to a country outside the EEA (third country) or to an international organisation transmission of data

169.The transfer of personal data, including the retransmission of personal data from a third country to another third country, which are or are intended to be subject to processing following their transfer to a third country or to an international organisation, may only take place if the Controller complies with, inter alia, the following conditions set out in Chapter V of the Regulation.

a) Transmission based on a conformity decision

The Controller will first check whether the European Commission has issued an adequacy decision for the country concerned. A transfer of personal data to a third country may take place without further authorisation if the Commission has determined that the third country, a territory or one or more specific sectors of the third country provide an adequate level of protection.

b) Data transmission with appropriate guarantees

Where there is no adequacy decision, the data may be transferred if the Controller provides adequate safeguards and the data subjects have enforceable rights and effective remedies.

Without specific authorisation from the supervisory authority, appropriate guarantees may include:

i. legally binding and enforceable instruments between public authorities or other bodies with a public-service mission;
ii. binding corporate rules;

iii. general data protection clauses adopted in accordance with the examination procedure;
an approved Code of Conduct, together with a binding and enforceable commitment by the third country controller or processor to apply appropriate safeguards, including with respect to the rights of data subjects;
v. an approved certification mechanism, together with a binding and enforceable commitment by the third country controller or processor to apply appropriate safeguards, including with respect to the rights of data subjects.

The Controller shall transfer personal data in the case referred to in point (iii) above both between controller and controller and between controller and processor using one of the model contracts specified by the competent body of the European Union.

For international data transfers to entities within a group of undertakings or the same group of undertakings engaged in joint economic activities, it is possible to apply binding corporate rules approved by the public authority, which provide adequate safeguards for the transfer as set out in point (ii) above.

In particular, the following may serve as appropriate safeguards, subject to the supervisory authority's approval:

contractual arrangements between the controller or processor and the controller, processor or recipient of personal data in a third country or within an international organisation; or
provisions between public authorities or other bodies with public-service mission to be incorporated into an administrative agreement, including provisions on the enforceable and effective rights of data subjects.

c) Derogations granted in special situations

In the absence of a decision of adequacy or appropriate safeguards, the transfer or multiple transfers of personal data to a third country or international organisation may only take place if at least one of the following conditions is met:

the data subject has given his or her explicit consent to the envisaged transfer after having been informed of the potential risks of the transfer due to the lack of a decision of adequacy and appropriate safeguards;
(ii) the transfer is necessary for the performance of a contract between the data subject and the controller or for the implementation of pre-contractual measures taken at the request of the data subject;
the transfer is necessary for entering into, or performance of, a contract between the controller and another natural or legal person which is in the interest of the data subject;
the transfer is necessary for important public interests;
the transfer is necessary for the establishment, exercise or defence of legal claims;
the transfer is necessary for the protection of the vital interests of the data subject or of another person and the data subject is physically or legally incapable of giving consent;
the transmitted data originate from a register which is intended to provide information to the public under Union or Member State law and which is accessible for consultation by the public in general or by any person having a legitimate interest therein, but only if the conditions for consultation laid down by Union or Member State law are fulfilled in the specific case.

IV. RESPONSIBILITY FOR DATA PROCESSING

IV.1. Responsibility of the Controller

170. The Controller is responsible for the processing of personal data.

171. In order to enforce his or her right to judicial remedy, the data subject may bring an action against the Controller or, in relation to processing operations within the scope of the Processor's activities, the Processor, before the data protection authority or a court, if he or she considers that his or her personal data are processed in breach of the provisions on the processing of personal data laid down by law or by a legally binding act of the European Union.

IV.2. Liability of the employee

172. The employee is liable under labour law, civil law and criminal law for the lawfulness of the data processing operations carried out in the course of his/her work and for compliance with the provisions of the Code.

173. Rules and the obligations under the law applicable to the processing of personal data.

V. RULES ON RECORD KEEPING

174. The Company shall ensure that the way and the content of personal data are recorded in accordance with the legislation in force.

175. The Company shall ensure appropriate logical and, where necessary, physical separation of processing for different purposes.

176. The Company manages electronic and paper records on the basis of uniform principles, taking into account the characteristics of the different data carriers. The principles and obligations under this Policy apply to both electronic and paper records.

177.The Company shall ensure, by means of the structure of the system of records, the definition of authorisations and other organisational measures, that the data contained in the records may be accessed only by employees and other persons acting in the interests of the Company who need to know them in order to perform their duties.

178.The Company shall provide access to the records to third parties acting as Processors who provide the Company with services related to the processing of data, subject to the requirement of data security.

179. The Company's electronic records comply with the requirements of data security, ensuring that data is only accessed for the purpose for which it is intended and only by those persons who need to have access to it in order to perform their duties.

V.1. Inventory of data assets

180.The Controller shall keep a register of the processing activities carried out by the Controller in accordance with Article 30 of the Regulation (inventory of data subjects), which shall contain all the purposes and processes of the Controller and their main characteristics.

181. The inventory of data assets shall include the following for each data processing operation:

a) the purpose of the processing;
b) the categories of personal data processed;
c) categories of persons concerned;
d) recipients;
e) the duration of the processing;
f) information concerning transfers to third countries or international organisations;

g) other comments.

182.Where the Controller carries out processing activities, it shall keep records of the processing activities carried out on behalf of its clients in accordance with Article 30 of the Regulation, which shall contain the following information:

a) the name and contact details of any controller for which or on whose behalf the Controller is acting as Processor and, where applicable, the names and contact details of the representatives of the Controllers acting as Processors and of their Data Protection Officers;
b) the categories of processing activities carried out on behalf of each Controller;
c) information concerning transfers to third countries or international organisations;
d) the date of conclusion of data processing contracts;
e) data security measures;
f) other comments.

183. The Company shall make the register available to the supervisory authority upon request.

V.2. Additional records

184. The Controller shall keep records of its data transfers, the Processors used, the exercise of data subjects' rights and data protection incidents.

185. The Controller shall keep a record of data transfers for the purposes of monitoring the lawfulness of the transfer and informing the data subject, which shall include:

a) the date of the transfer of the personal data which it processes,
b) the purpose and recipient of the transfer;
c) the scope of the personal data transferred and the data subjects concerned;
d) the means and channel of transmission; the identity of the person transmitting the data; and
e) other data specified in the legislation providing for the processing.

186. The Controller keeps a register of its Processors, which contains the following characteristics of the processing:

a) the purpose of the processing to which the Processor is contributing;
b) Processor details;
c) the scope of the data to be processed;
d) the characteristics of data processing;
e) whether the Processor uses an additional Processor, and if so, the details of that Processor.

187. The records concerning the exercise of the rights of the data subject and the execution of the related requests include:

a) personal data concerning the data subject;
b) whether or not it has been identified;
c) the subject of the request (name of the right exercised);
d) the date of receipt of the application;
e) the deadline for complying with the request;
f) the way and channel for submitting the request;
g) the action taken on the request;
h) the date of execution of the request;
i) the date on which the information on the action taken on the request was provided to the data subject.

188. Where the data subject has requested the erasure of his or her personal data, subsection (a) of the register referred to in point 201 shall be erased.

189. The Controller shall keep a record of the data protection incidents, indicating the main facts and circumstances relating to the data protection incident as follows:

a) the date of occurrence;
b) the deadline for notification;
c) the nature of the damage;
d) type of incident;
e) description of the incident;
f) the impact of the incident on the data subjects;
g) the number of persons concerned;
h) categories of persons concerned;
i) the scope and number of personal data concerned;
j) the consequences of an incident;
k) measures taken to remedy the consequences of the incident;
l) whether and when the data subjects have been informed;
m) other comments.

V.3. Keeping of records

190. The registers in force at the date of entry into force of these Rules are referred to in Rules XI. chapter.

191. The administrator is responsible for the accuracy and updating of the records.

192. The records shall be kept in paper and/or electronic form, as directed by the administrator, in accordance with the data security rules set out in these Rules.

193. The keeping and updating of the records is the responsibility of the administrator on the basis of the information provided by the relevant departments (if the work is split into departments within the Company) or the employee who is actually processing the data.

194. The manager is responsible for checking that the records are accurate and kept up to date.

195. Employees must immediately notify the person(s) responsible for keeping the register, either directly or through the relevant departmental managers (if the work is split into departments within the Company), whenever an event occurs in the course of their work that affects the data content of the register.

VI. THE DATA BREACH

VI.1. Occurrence of a data protection incident

196. In the event of a breach of data security or accidental or unlawful destruction, loss, alteration, unauthorized disclosure or transmission of personal data processed by the Controller, or unauthorized access to such data (hereinafter referred to as a "data breach"), the Controller or the person processing personal data processed by the Controller under any legal relationship shall, in the event of a data breach as defined by the Controller, follow the procedure set out in Section X. in Chapter X of the relevant internal rules of procedure.

VII. IMPACT ASSESSMENT

VII.1. Conduct an impact assessment

197. Where a processing operation envisaged by the Controller is likely to present a high risk to the rights and freedoms of natural persons, taking into account its nature, scope, context and purposes, the Controller shall carry out an impact assessment prior to the processing operation, in which case the relevant internal rules of procedure referred to in Chapter X of this Policy shall be followed.

198. An impact assessment shall be carried out in particular in the following cases:

a. the processing is intended to provide a systematic and extensive assessment of certain personal aspects relating to natural persons based on automated processing, including profiling, and on which decisions which produce legal effects concerning a natural person or similarly significantly affect a natural person are based;
b. the processing of a large number of special categories of personal data referred to in point II.11 of these Rules or personal data relating to decisions on criminal liability of the data subject and to criminal offences; or
c. large-scale, systematic surveillance of public places.

199. In addition to the above, an impact assessment must also be carried out for additional data processing operations specified by the NAIH.

200. The impact assessment shall cover at least:

a. a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interests pursued by the controller;
b. to assess the necessity and proportionality of the processing operations in the light of the purposes of the processing;
c. to assess the risks to the rights and freedoms of the data subject; and
d. describe the measures taken to address the risks, including safeguards, security measures and mechanisms to protect personal data and to ensure compliance with this Regulation, taking into account the rights and legitimate interests of data subjects and other persons.

201.The Controller shall, where appropriate, without prejudice to the protection of commercial interests or the public interest or the security of processing operations, seek the opinion of the data subjects or their representatives on the envisaged processing.

202.If the data protection impact assessment concludes that the processing is likely to result in a high risk in the absence of measures taken by the Controller to mitigate the risk, the Controller shall consult the supervisory authority before processing the personal data.

203. The controller shall, as appropriate, and at least in the event of a change in the risk posed by the processing operations, carry out an audit to assess whether the processing of personal data is carried out in accordance with the data protection impact assessment.

VIII. OTHER RULES CONCERNING THE PROCESSING OF PERSONAL DATA

VIII.1 Characteristics of each data management purpose and activity; introduction of new data management purposes or processes

204. The detailed rules of the processing operations related to each of the processing purposes of the Controller are set out in the processing notices published by the Controller. The Controller shall carry out its processing activities in relation to each processing purpose as described in the Data Processing Notices.

205. Data processing notices drawn up in relation to specific processing operations shall be deemed to be published without any further action or provision, after obtaining the necessary approvals, after signature by the Controller and publication in a manner appropriate to the specific processing operation. The Controller shall keep a register of the applicable privacy notices as set out in Chapter V.

206. The introduction of a new data management process or the modification of an existing data management process may only be ordered by the administrator.

207. An employee who has a need to introduce a new data management process in connection with the performance of a task related to his or her job shall notify the head of the department (if the work is split into departments within the Company), who shall notify the CEO. If the work is not divided into departments within the Company, the employee shall inform the Managing Director directly.

208. An employee who has a need to change the data management process concerning his or her job shall notify the head of the department (if the work is split into departments within the Company), who shall notify the CEO. If the work is not divided into departments within the Company, the foreman shall inform the Managing Director directly.

209. A new data processing process or a change to data processing processes will be introduced if it does not conflict with the provisions of the Code.

210. Before introducing a new data management process or changing data management processes, it is necessary to define the main features of data management, in particular:

a) the purpose of the processing;
b) whether that purpose can be achieved by another processing operation;
c) the legal basis for the processing;
d) the persons concerned;
e) the scope of the data relating to the data subjects;
f) the source of the data;
g) the duration of the processing of the data;
h) the type of data transferred, the recipient and the legal basis for the transfer, including transfers to third countries;
i) the name and address of the Controller and the Processor, the place of actual processing and the activities of the Processor in relation to the processing;
j) the nature of the data processing technology used.

211. When introducing a new data processing process or changing an existing data processing process, the administrator shall ensure that contracts, records and policies relating to the processing of personal data are updated and that the amended and updated data protection documents are made available to the relevant persons. The activities under this point shall be documented in a verifiable manner.

IX. REMEDIES

IX.1. Data subjects' rights of redress

212. The data subject may contact the Controller with any questions, comments, requests or complaints regarding the processing of his or her personal data at the e-mail address indicated in the information notice on the processing activities, or by post or in person at the registered office of the Controller. In such a case, the Controller shall investigate the matter within a maximum of 30 (thirty) days and inform the data subject of the outcome of the investigation.

In addition to the provisions set out in the previous point, any person may initiate an investigation against the Controller at the NAIH on the grounds that a violation of rights has

occurred or is imminent threat thereof in connection with the processing of personal data, or that the exercise of his or her rights of information, access, rectification, restriction, erasure, or remedy is restricted by the Controller or that his or her request to exercise such rights is rejected. The notification can be made using one of the following contact details:

National Authority for Data Protection and Freedom of Information (NAIH)

- Postal address: 1363 Budapest, Pf. 9.
- Address: 1055 Budapest, Falk Miksa utca 9-11.
- E-mail: ugyfelszolgalat@naih.hu
- URL: http://naih.hu

214. In addition to points 212 and 213, in order to exercise his or her right to judicial remedy, the data subject may also have recourse to the courts if he or she considers that the controller or the processor on his or her behalf or under his or her instructions is processing his or her personal data in breach of the provisions of the law or of a legally binding act of the European Union relating to the processing of personal data. The action may also be brought, at the choice of the data subject, before the courts for the place where the data subject resides or is domiciled or before the courts for the place where the controller is established.

X. CODES OF PRACTICE, RULES OF PROCEDURE

- Privacy Incident Policy and Procedure
- Policy and procedure for responding to a request for information
- Data Protection Impact Assessment Policy

XI. DISCLOSURES

- Data Asset Inventory
- Register of applications and exercises of rights
- Data transmission register
- Data protection incident record
- Register of Processors
- Article 30 register kept as a Processor
- Data management information
- Privacy notices in force

XII. FINAL PROVISIONS

215. The administrator shall ensure that the Staff are promptly made aware of the Rules and that the Staff accept them as binding on them,
that all employees of the Company will be notified by e-mail following the signing (acceptance) of the Code.

216. All applicable internal rules, including these Rules, are available and may be consulted by any employee of the Company at the Company's headquarters.

217. The administrator shall ensure that all staff members act in accordance with the rules set out in the Code.

218. For new Employees joining the Company after the entry into force of the Rules, the Rules are available at the Company's head office and the Human Resources Officer will explain the Rules to the new Employee upon joining the Company.

219. These Rules shall enter into force on the date of signature. Upon the entry into force of these Rules and Regulations, consolidated with the amendments, the previous Rules and Regulations shall be repealed.

220. After the entry into force of these Rules, the Controller shall act on the basis of the provisions of the applicable data protection legislation in force at the time and the provisions of these Rules not affected by the amendment of the applicable legislation until the amendment of the applicable data protection legislation affecting certain provisions of these Rules is incorporated into these Rules.