PRIVACY POLICY

Centre for Agricultural Research, Hungarian Academy of Sciences

Martonvásár

2018.

I. Introduction, Principles, Scope of the Prospectus

The Hungarian Agricultural Research Center (headquarters: Martonvásár 2462, Brunszvik street 2, statistical number: 15300519-7219-342-07, tax number: 15300519-2-07, e-mail: atk@agrar.mta.hu, tel .: +36 22 569 500, Fax: +3622460213, website: www.agrar.mta.hu, represented by Ervin Balázs Director General, hereinafter "Data Controller") as Data Controller in the processing of personal data by the European Parliament and the Council) on the protection of natural persons with regard to the processing of personal data and on the free movement of such data by 2016/679. of the Act of 27 April 2016 (hereinafter referred to as "the Regulation" or "the GDPR Regulation") and the relevant laws.

The Data Controller respects the rights of the "Affected" personal data. This Prospectus summarizes in a concise, simple manner how the Data Handler collects, how to use it, as well as explains the data used by the Data Handler and the privacy and enforcement rights of the Affected Data Protection.

Detailed regulation is required for further information requirements contained in this Decree and related acts, or to contact the Data Handler at the contact details provided in this Prospectus.

The purpose of this Prospectus is to ensure that the Data Controller ensures the protection of the constitutional principles of data protection, data security requirements, prevents unauthorized access to and unauthorized alteration, loss or disclosure of data.

In the course of its data management, the Data Controller shall act in accordance with the following principles:

In data management time, before the data processing begins, you inform the Affiliate of the data management rules as required.

The Data Controller collects, stores and uses only personal data in accordance with the requirements of the purpose of data management.

Collected personal data is always relevant, relevant and appropriate to the given purpose, keeping the Data Manager in compliance with the principle of data saving.

In the interest of data accuracy, the Data Handler takes reasonable steps to ensure that the personal data of the Person concerned are complete, accurate, up-to-date and reliable to the extent appropriate for the purpose.

The Data Handler uses personal data for marketing purposes solely with the consent of the Affected Person and allows such communication to be prohibited by the Affected Person.

The Data Manager shall take proportionate and complete steps to ensure the protection of the personal data of the Person concerned, as detailed in this Privacy Statement, including cases where they are transmitted to third parties.

The scope of this Prospectus covers the entire data management activity of the Data Controller and, accordingly, extends - explicitly but not exclusively - to the Data Manager with the Data Manager the contact persons, employees, members of the business and other organizations and partner institutions in contact with the economic (business) agents, etc. (Jobseekers / Applicants) to manage your personal information, including the use of the www.agrar.mta.hu website as well as the use of institutional websites, data management related to the electronic observation system operated by the Data Controller and the data security principles applied .

II. Interpretative provisions

• Regulation, GDPR Regulation: Regulation No 2016/679 on the protection of individuals with regard to the processing of personal data and on the free movement of such data by the European Parliament and the Council (EU) (27 April 2016);

• Infotv: CXII. law on information self-determination and freedom of information;

• December: XXXIII. Act on the Status of Civil Servants

• Company name: CXXXIII. Act on the Law on the Protection of Persons and Property, and the Act on Private Investigations;

• Art.:2017. CL. law on taxation;

• Sztv.:2000. Act C of Act C on Accounting;

• VAT: CXXVII of 2007. Act on General Sales Tax;

• Civil Code: Act V of 2013 on the Civil Code;

• **Personal data** - Any information about an identified or identifiable natural person ("concerned"); a natural person may be identified, directly or indirectly, based on one or more factors relating to the physical, physiological, genetic, intellectual, economic, cultural or social identity of an identifier such as name, number, positioning data, online identifier or natural person identified;

• **Specific data**: Personal data related to racial origin, nationality, political opinion or party affiliation, religious or other beliefs, membership of an interest representation organization, personal data relating to sexual life, personal data relating to health status, abnormal passion, as well as criminal personal data.

• **Genetic data**: any personal data relating to the inherited or acquired genetic characteristics of a natural person that carries specific information on the physiology or health of the individual resulting from an analysis of the biological sample taken from that natural person;

• **Biometric data**: personal data derived from any specific technical procedures relating to the physical, physiological or behavioral characteristics of a natural person that allows or confirms the unique identification of a natural person such as facial or dactyloscopic data;

• **Health Data**: personal data relating to the physical or psychological health of a natural person, including data relating to health services provided to a natural person that carries information on the health of a natural person;

• **Data management** - any operation or operation in any automated or non-automated way of personal data or data files, such as collecting, capturing, rendering, compiling, storing, modifying or modifying, querying, inspecting, using, communicating, distributing or otherwise disclosure, coordination or interconnection, restriction, deletion or destruction;

• **Data Administrator** - a natural or legal person, public authority, agency or any other body that determines the purposes and means of handling personal data individually or with others; where the purposes and means of data management are defined by Union or national law, the data controller or the particular aspects of the designation of the data controller may also be defined by Union or national law;

• **Data processor** - a natural or legal person, public authority, agency or any other body that handles personal data on behalf of the data controller;

• **Registering of data records**: a register of data management activities carried out by the Data Controller, containing the data management data, the purpose of the data management, the categories of persons concerned, the categories of personal data processed, if possible, the addressees to whom the data will be communicated, the name and contact details of the data processor (s) and, where possible, the deadline for deleting the individual data categories,

• **Recipient** - a natural or legal person, a public authority, agency or any other body with whom or with which personal data is communicated, whether or not it is a third party. Public authorities which have access to personal data in an individual investigation in accordance with EU or national law are not considered recipients;

• **Third Party** - a natural or legal person, a public authority, an agency or any other body that is not the same as the data subject, the data controller, the data processor or any person authorized to manage personal data under the direct control of the data controller or data processor ;

• **Contribution of the person concerned** - a voluntary, concrete and informed and explicit statement of the will of the person concerned by which he or she indicates the statement in question or a statement of unambiguous effect by confirming his consent to the processing of personal data concerning him;

• **Event that violates data protection**: Computer Error, Data Protection Incident.

• **IT Failure**: Disruption to work, disruption of work, disruption of service, discontinuation of service, which is not a data protection incident in the operation of the IT system, but the security, integrity or availability of the IT system may be jeopardized;

• **Privacy incident**: Damage to security resulting in accidental or unlawful destruction, loss, alteration, unauthorized disclosure or unauthorized access to personal data transmitted, stored or otherwise handled;

• **Privacy Officer**: Person designated by the Organization pursuant to Article 37 (1) (a) of Regulation (EU) 2016/679 of the European Parliament and of the Council (GDPR Regulation) whose contact details and status are contained in this Prospectus

• **Authority**: National Data Protection and Information Security Authority, www.naih.hu

• **other websites in the constituency of the institute**:
o mta-taki.hu
o www.rissac.hu
o http://www.csalomoncsapdak.hu/
o http://www.proplanta.hu/

III. Data management (service provider) data and contact details

Data Controller Name: Agricultural Research Center, Hungarian Academy of Sciences

Headquarters: 2462 Martonvásár, Brunszvik u. Second

Privacy Officer: **dr. András György**

E-mail: adatvedelem@agrar.mta.hu

Tel .: +36 22 569 500

Fax: +3622460213,

Website: www.agrar.mta.hu

The data protection system of the data controller, the legal status of the Data Protection Officer

The current Director-General of the Data Controller determines the conditions of data protection, the data protection and the related tasks and responsibilities, taking into account the specificities of the Data Management Organization.

The Data Processing staff ensures that unauthorized persons can not access personal data and that personal data are stored and stored in such a way that the unauthorized person can not be accessed, identified, changed or destroyed.

The data controller's data protection system is supervised by the Director-General through a Data Protection Officer appointed or entrusted by him.

The Data Protection Officer shall be appointed on the basis of professional competence and, in particular, knowledge of the law and practice of data protection, as well as the ability to perform data management.

The Data Protection Officer may also be an employee of the data controller, but may also perform his / her duties under a service contract.

The Data Administrator shall make the name and contact details of the Data Protection Officer available in this Policy and on its website and shall be notified to the competent Supervisory Authority (NAIH).

The data controller must ensure that the Data Protection Officer intervenes in an appropriate manner and in a timely manner in all matters relating to the protection of personal data. It must be ensured that the resources necessary to maintain the expert knowledge of the Data Protection Officer are available.

The Data Protection Officer can not accept instructions from anyone regarding the performance of his / her duties. The Data Controller may not release the Data Protection Officer in connection with the performance of his or her duties and shall not penalize it. The Data Protection Officer is directly responsible to the Director-General.

The Affected Person may contact the Data Protection Officer for all matters relating to the handling of their personal data and the exercise of their rights.

The Data Protection Officer is bound by the obligation of confidentiality regarding the fulfillment of his duties.

The Data Protection Officer may also perform other duties, but there is no conflict of interest with regard to the duties provided by the Director-General

Balancing Interests

The Data Handler records the following rules for data management without consent, which the Data Controller may exceptionally have in the interests of a third party's legitimate interest.

If the legal basis is defined in Article 6 (1) (f) (ie a legitimate interest) of the GDPR, the data processing process becomes lawful and insofar as it is necessary to enforce the legitimate interests of the Data Controller or a third party unless these interests the interests or fundamental rights and freedoms of the person concerned, which require the protection of personal data.

In order to examine the lawfulness of data processing, the Data Controller performs an interest weighing test in which case the need for the purpose of data management and the proportionate limitation of the rights and freedoms of the data subjects are properly substantiated.

In the Interest Weighing Test, the Data Handler identifies its legitimate interest in data handling as well as the stakeholder's interest in the weighting and the relevant fundamental right. The condition of the weighting of conflicting rights and interests is always examined by the Data Controller in view of the specific circumstances of the particular case. In the weighing process, the Data Handler takes into account, in particular, the nature and sensitivity of the data being handled or to be handled, the extent of its publicity, the gravity of the potential violation, etc.

Right to Data: The data handler submits the data to the customer service, to the employee performing the data management activities, and to the employee and data processor as the recipient of accounting and taxation tasks.

VI. data Security

The Data Manager is Info TV. as well as your obligation under the GDPR to take care of the security of your Affected Data, take the necessary technical and organizational measures and establish the procedural rules that apply to Info Info, GDPR, and other data - and to enforce secrecy rules. Access data stored in the Data Manager's database may only be accessed by the Data Manager's authorized personnel.

The so-called " cloud computing applications are also part of it. Cloud applications are typically of an international or cross-border nature and, are used for data storage when the data center / organization computer center is not the data storage server, but a server center that can be located anywhere in the world. The main advantage of cloud applications is that they provide substantially independent, highly secure and flexible storage and processing capacity from a geographic location.
The Data Controller selects partners with cloud computing with the utmost care, makes every effort to conclude a contract that is in the interest of the data security interests of the Affiliates, to be transparent to their data management principles and to check data security regularly.

It is possible that a reference to the Data Handler's website is linked to pages maintained by other providers (including buttons, logos for sign-in, sharing options), where the Data Controller has no influence on personal data management practices. The Data Handler draws the attention of those concerned that if they click on such links, they can be transferred to other service providers. In such cases, we recommend that you read the validation information that applies to these pages. This Privacy Statement applies only to data management by the Data Controller. If you modify, delete, disclose any of your data on the affected external website, it will not affect the data management by the Data Handler, you must also make such modifications on the Website.

Physical protection

For the security of personal data handled on paper, the Data Handler applies the following measures:

- data can only be accessed by authorized persons, others can not access it, may be disclosed to others;

- documents must be placed in a well-sealed, dry, fire-proofing and property protection facility;

- the files in continuous active treatment are only available to the competent authorities;

- a data collector who manages data management during the day can only leave a room where data management is being carried out to close the storage media or to close the office;

- the Data Handler's Data Processing Officer closes the paper-based media at the end of the work;

- if the personal data handled on the paper is digitized, the Company applies the security rules applicable to digitally stored documents.

IT protection: Information Protection is provided by the Data Controller as per the current IT Security Code.

Access management:

The Data Handler has established a centralized rights management rule system and applies it to ensure that all users in the (IT) systems operated by the Data Controller cover all phases of the user access lifecycle (from the first registration of new users to the final deletion from the register) access to the user interface that is required to perform the job and to define the general requirements for access control of information and information systems operated by the Organization, a fundamental requirement for the latter to be able to ascertain when, within and outside the Organization applications / systems.

In the use of the IT systems / applications it operates, the Data Controller also ensures the protection of data protection principles, data security requirements, and prevents unauthorized access or change of data and unauthorized disclosure, while ensuring that users are able to perform their workflow you actually have access to the tools and information you need to accomplish each task.

The detailed rules of privilege management are contained in the Data Controller's Voyage Privacy Policy.

Incident management

The Data Handler's Incident Management Policy sets out the procedures for dealing with acts that violate data protection, the responsibilities and the necessary procedural order.

Through incident management, the Data Controller facilitates the handling of events that violate data protection related to its operation in a unified system, to prevent the occurrence of acts that violate the data protection, and in the event of its occurrence, if necessary, to establish responsibility and to take measures. The Incident Management Code sets out the concepts, procedures, and measures that will prevent the occurrence of data corruption-related incidents occurring during the operation of the Data Manager and the management of the detected events.

IV. The purpose of data management, the scope of the data being processed, the duration of the data management, and the access to data concerning the Users involved in the Data Manager's services at the data manager's events, are available at www.agrar.mta.hu

<u>Purpose and legal basis of data management</u>

Data handler is the person in charge of the conclusion and performance of the contract (in which the Affected is one party), and a legitimate interest in the following cases: intention to conclude contracts, performance of contract (conduct of research and investigation on order,

sale of online publications, provision of accommodation services, organization of events, provision of library services, Visitor Center).

The Data Controller manages the Personal Data in compliance with a legal obligation to comply with legal obligations in the following cases: fulfillment of billing, accounting, accounting obligations (Art.

The data handler handles personal data on the basis of the express and voluntary consent of the Affected Person in the following cases: Newsletter, Event and Conference Invitation, Contact - Responding to a Web Site Interpretation, Marketing Goal, Recognizing and Collecting Visitors' Habits - Anonymous User IDs cookie)

The data storage method is both electronic and paper based

The Data Controller records that visitors to the Website, using the Website (without contacting the Web), collect and manage data using anonymous User IDs (cookies or cookies) and their acceptance by the Target. The essentials of cookies are summarized below in the Data Handler.

The Data Manager is a variable content alphanumeric information that is stored on the user's computer and which can be stored for a period of validity for a period of validity, for example, cookies or cookies for the services and the Website.

A cookie is a sequence of characters that can be used to identify and store profile information that the service providers place on your affected computer. It is important to know that such a sequence of characters is not capable of identifying the Person in any way, but it is only capable of recognizing the affected computer. Personally-related information and personalized service in the Internet world of the Internet can only be provided if service providers can uniquely identify their customers' habits and needs. Service providers are trying to identify anonymously so that they can learn more about customer information usage habits to further improve the quality of their services and, on the other hand, offer customization options to their customers.

For example, cookies are used to store the Preferences preferences and settings; these will help you sign in; you can display and analyze personalized ads for your site. To do this, you can use Data Management Services to collect and track information on relevant activities such as relevance, referrals, searches, openings, key and most commonly used features.

Flash cookies are used by website operators to tell you, for example, whether the user has ever visited the website or help identify the features / services that the person most interested in may be interested in. Search and Flash cookies increase your online experience by retaining the information you prefer to the Affinity while you are on a page. Neither the search engine nor the Flash cookies can identify the Person personally, and the Affected person can reject browser cookies through the browser settings but will not be able to take advantage of all the features of the web site without such cookies.

If you do not want this ID to appear on your computer, it is your way to configure your browser so that it does not allow the unique identifier to be placed on it, and you have the right to cancel your permission at any time, to delete the unique ID, but in this case it is possible that the services will not or will not be in the form of Affected as if you were allowed to locate the IDs.

Services are used by a large number of users in a variety of software and hardware environments with different uses and scope. The development of services can best be tailored to the needs and opportunities of users whenever the website operator gets a comprehensive

view of their usage habits and needs. However, because of the large number of users, personal access and feedback is an effective complementary method, when their routines and services run environment data are collected and analyzed by an automated method for the site's operator.

The aim of the data management is to ensure the proper and high quality operation of the website, to monitor and improve the quality of Data Management services, to identify malicious visitors visiting the site, and to measure attendance.

They are entitled to know the data: staff responsible for the supervision and maintenance of the Data Management's IT system and possible data processors

V. The purpose of data management, the scope of the data to be processed, the duration of the data management, and the knowledge of the data are entitled to the data controllers contacting agents (eg individual entrepreneurs, etc.) in contact with the data manager, as well as business associates, employees, agents, in respect of

The purpose and legal basis of data management

The data controller handles personal data in a legitimate interest in the following cases: intent to contract, conclusion and performance of a contract, security function: home / site surveillance.

The Data Handler manages your personal information on the basis of your explicit and voluntary consent by you, in the following cases: Sending a Bulletin (Marketing).

The scope of the data processed, the duration of data management, and the ability to access the data

By referring to the claimed legal basis, the Data Controller collects and manages the personal data according to the following table (s): - Retention time:

- **Legitimate interest-based data**: Name, email address, phone number; In case of partner contacts: position in partner company. In case of employees who work directly or indirectly to the data controller, depending on the quality of the person concerned: citizenship, place of birth / place of residence, address (domicile) tax number, CV, work experience, education / training, language skills, pictures, video and sound recording. Retention time according to the performance of the contract or the termination of legitimate interest or the related statutory provision (Article 6: 22) 5 years. Recording security camera: In the absence of any usage recorded in the Rules of Use of the Szvtv or the Data Controller's Electronic Monitoring System, 3 working days from the recording (Section 31 Paragraph 2 of the Szvtv)
- **Data handled by the affected volunteer** (The method of withdrawal of the contribution concerned is provided in Chapter XIII of this Prospectus): Name, email address, phone number, contact details - position at partner company: Retention time until unsubscription, until withdrawal of consent
- **In the case of research** and investigation activities and ordering of publications: address, tax identification number / tax number, mother's name, place of birth / time, registration number and registered office of individual entrepreneur, bank account number, delivery address, delivery name, billing name, billing address
- **In the case of providing accommodation services**: Full name, Arrival date, Arrival date, Departure date, Number of adults in a room, Email address, Full mailing address, Comments - any preferences

- **In case of visitors to the Visitor Data processed on the basis of a statutory requirement (fulfillment of a legal obligation):** Accounting records (Accounting Act. Under Section 169 (2), at least eight years) Center: Name, Vehicle registration number

VII. Access, modification, correction and portability of personal data

Access

You are entitled to receive feedback from the Data Handler as to whether your Personal Data is being processed and, if such processing is in progress, you have the right to access Personal Data and the following information:

1.1. the purposes of data management;

1.2. the categories of personal data concerned;

1.3. the categories of recipients or recipients with whom or with whom the Personal Data will be communicated or communicated

Amendment, correction

The Affected person is entitled to request a Data Manager to correct, without undue delay, any inaccurate Personal Data on his request. Taking into account the purpose of data management, the Affected person is entitled to request the supplementation of incomplete Personal Data, including by means of a supplementary statement.

Portability

You have the right to receive personal data provided to you by a Data Controller in a machine-readable, widely used, machine-readable format, and have the right to transmit this data to another Data Manager without this being obstructed by the Data Controller whose Your Personal Information is available to you when:

3.1. data management is based on a voluntary contribution or a contract where the Affected is one party; and

3.2. data management is done automated

VIII. The deletion, limitation and privacy of personal data

Deletion

You are entitled to request that Data Administrator, without undue delay, disclose any personal data relating to you, and that Data Manager is obliged to delete Personal Information about the Affiliate without undue delay if one of the following reasons exists:

the Personal Data is no longer required for the purpose for which they have been collected or otherwise handled;

- Has contacted the Customer Service through the voluntary consent of the data controller and has no other legal basis for data processing;
- Has been concerned with data handling for reasons related to his / her own situation or because of direct business information management and has no prior legitimate reason for data handling;
- the personal data has been unlawfully handled;
- the Personal Data shall be deleted from the Data Actor's legal obligation as provided for by the law of the Union or of the Member States;

- the collection of Personal Data was made directly to the provision of information society services for children.

If the Data Controller has disclosed the Personal Data and is required to cancel it under paragraph 1, taking reasonable steps, including technical measures, to take account of the available technology and implementation costs in order to inform the data controllers handling the data that the Target has requested they will either delete the duplicate or duplicate of the links to the Personal Data in question or of this Personal Data.

You may revoke your consent for data management at any time by submitting a statement to the Data Controller or the Data Protection Officer. The withdrawal of the consent does not affect the lawfulness of the data handling prior to the withdrawal.

Paragraphs 1 and 2 shall not apply where data processing is required:

- to exercise the right to freedom of expression and information;
- the fulfillment of an obligation under EU or Member State law for the processing of personal data for the Data Controller and for the performance of a task in the exercise of public authority exercised in the public interest or in the exercise of a public authority exercised on the Data Controller;
- public interest in the field of public health or public health;
- For purposes of public interest archiving, for scientific and historical research purposes or for statistical purposes, where the law referred to in paragraph 1 is likely to render impossible or seriously jeopardize this data management; or
- filing, enforcing or protecting legal claims

Restriction

You have the right to request a Data Controller to restrict the processing of data on request if one of the following is true:

- (a) The person concerned disputes the accuracy of the Personal Data; in this case, the restriction concerns the period of time that Data Manager can verify the accuracy of Personal Data;
- (b) data processing is unlawful and Affected opposes the deletion of data and instead asks for their use to be restricted;
- c) The Data Controller no longer needs Personal Data for Data Handling, but the Requested Party requests them to submit, enforce, or protect legal claims; or
- d) He has objected to data handling for reasons related to his / her own situation; in this case, the restriction applies to the duration of determining whether the rightful reasons of the Data Manager have priority over the legitimate grounds of the Affected Person.

If the processing of data is subject to limitation under paragraph 1, such Personal Data may only be used with the consent of the Person concerned or with the submission, enforcement or protection of legal or other rights of the natural or legal person, important public interest.

The Data Controller who has restricted the processing of data at the request of that person pursuant to paragraph (1) shall inform the prior notice of the discontinuance of the restriction of the data handling.

Protest

You are entitled to object to the handling of your Personal Information for any reason relating to your own situation if you are required to perform a task under the exercise of a public authority on the Data Controller or to manage the legitimate interests of the Data Controller or a third party, including profiling based on those provisions. In this case, the Data Controller may not process Personal Data unless the Data Controller proves that data management is

justified by legitimate reasons of enforceability that prevail over the interests, rights and freedoms of the data subject, or for the submission, enforcement or protection of legal claims related.

If your Personal Data is handled for direct business acquisition, you are entitled to at any time object to the handling of Personal Data for that purpose, including profiling, if it is related to direct business acquisition.

If the Customer objects to the handling of Personal Data for direct business acquisition, Personal Data may no longer be handled for that purpose.

Procedure for exercising the right of access

You may at any time request an interested party to provide information about your rights under this Regulation or about data handling for the data subject by submitting a request to the Data Controller or the Data Controller's Data Protection Officer.

The application must be submitted in writing electronically or on a paper basis

If the Request Form is not returned by the person concerned and therefore the person concerned can not be identified and can not be fully assured that the person concerned asks for information relating to the processing of data concerning himself / herself or his agent, the request must be rejected, the reason for the refusal with the applicant communicated.

In the case of a civil servant concerned with the data controller, the identification can also be carried out in the absence of a request form.

User Enforcement Opportunities

In the event of violation of his or her personality rights and in the cases specified in the Decree, the User may request the assistance of the National Privacy and Data Protection Authority and shall have the right to initiate a lawsuit before the court of his / her place of residence or residence:

Name: **National Data Protection and Freedom Authority**

Postal address: 1530 Budapest, Pf .: 5.

Address: 1125 Budapest, Szilágyi Erzsébet fasor 22 / c.

Phone: +36 (1) 391-1400

Fax: +36 (1) 391-1410

Web: naih.hu

E-mail: ugyfelszolgalat@naih.hu

Changes of information, entry into force

The Data Controller reserves the right to modify or update this Prospectus at any time, without prior notice, and to publish the updated version on its web pages. Any modification applies only to Personal Data collected after the publication of the revised version.

This Prospectus will enter into force on the date of its publication, which will terminate the Data Handler's previous Data Handling Notice at the same time.