

## Data Management Policy

### Introduction

This Data Management Policy (hereinafter referred to as: **the Policy**) applies to data management and data processing activities pursued by **IFKA Public Benefit Nonprofit Ltd.** (hereinafter referred to as: **IFKA**), responsible for the GINOP – Economic Development and Innovation Operational Program number **GINOP-1.1.4-16-2017-00001**<sup>1</sup>, otherwise known as the “**Future Hungarian Multinationals I - For the identification, assessment, motivation and definition of development needs of high growth potential small and medium-sized businesses**” (hereinafter referred to as: **Future Hungarian Multinationals**) in the course of implementation of the **Future Hungarian Multinationals**.

Data management activities of IFKA not pertaining to the Future Hungarian Multinationals (hereinafter referred to as **Other Data Management**) are only covered by this policy if IFKA explicitly so stipulates.

The official website of the Future Hungarian Multinationals can be reached at **<https://mmp.ifka.hu>** and is operated by IFKA. The data controllers of the Future Hungarian Multinationals are IFKA (hereinafter referred to as: the **Data Controller**) and the following additional co-operating parties are **data processors**.

Participation in the Future Hungarian Multinationals is open to businesses that meet the criteria set forth in Section (1) of §3 of Act XXXIV of 2004 on small and medium-sized enterprises and aid for their development (hereinafter referred to as: the **SME Act**). Accordingly, the implementation and operation of the Future Hungarian Multinationals is not aimed expressly at managing data of private individuals. The Data Controller shall endeavor to limit the scope of managed data to corporate data and shall deal with personal data only when indispensable.

When processing private individuals’ data in the course of operating and implementing the Future Hungarian Multinationals, the Data Controller and the data processors shall do so in a trustworthy manner and in good faith, thus performing all obligations and ensuring all rights that serve to protect data subjects’ data security, applicability and exercising of their related rights in the data processing process.

### Aim of the Policy

The purpose of this Policy is to ensure that during the operation and implementation of the Future Hungarian Multinationals, the data of private individuals interacting with IFKA is handled within a suitable legal framework, primarily 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: **GDPR**), as well as Act No CXII of 2011 on the right to informational self-determination and freedom of information <sup>1</sup> GINOP [Economic Development and Innovation Operational Program] Managing Authority: Ministry of Finance, Deputy State Secretariat for the Implementation of Economic Development Programs

(hereinafter referred to as: the **Information Act**), as well as all other mandatory legal norms applicable to data processing.

## **Legal Background**

When drafting the Policy, the Data Controllers primarily worked on the basis of the **GDPR** and the **Information Act**, Act V of 2006 on public company information, company registration and winding-up proceedings (**Registration Act**), Act V of 2013 on the Civil Code (**Civil Code**), along with all other legal norms containing mandatory data processing provisions.

## **Details of Data Controller and data controllers**

### **Data Controller's details**

Name of Data Controller: **IFKA Public Benefit Nonprofit Ltd.**

Official Seat: 1062 Budapest, Andrásy út 100.

Phone Number: +36 (1) 213 2213

Email Address: [info@ifka.hu](mailto:info@ifka.hu) Website: [www.ifka.hu](http://www.ifka.hu)

### **Data processors' details**

Name of data processor: **Ministry of Finance**

Official Seat: 1051 Budapest, József nádor tér 2-4.

Phone Number: +36 (1) 795 1400

Email Address: [ugyfelszolgalat@pm.gov.hu](mailto:ugyfelszolgalat@pm.gov.hu)

Website: <https://www.kormany.hu/hu/nemzetgazdasagi-miniszterium>

Name of data processor: **Ministry of Foreign Affairs and Trade**

Official Seat: 1027 Budapest, Bem rakpart 47.

Phone Number: +36 (1) 458 1000

Email Address: [kozkapcsolat@mfa.gov.hu](mailto:kozkapcsolat@mfa.gov.hu)

Website: <https://www.kormany.hu/hu/kulgaszdasagi-es-kulugyminiszterium>

Name of data processor: **HEPA Hungarian Export Promotion Agency Nonprofit Zrt.**

Official Seat: HEPA Hungarian Export Promotion Agency Nonprofit Zrt.

Phone Number: +36 (1) 922

2600

Email Address: [info@hepa.hu](mailto:info@hepa.hu)

Website: <http://hepa.hu/>

Name of data processor: **Ministry for Innovation and Technology**

Official Seat: 1011 Budapest, Fő utca 44-50.

Phone Number: +36 (1) 795 1700

Email Address: [ugyfelszolgalat@itm.gov.hu](mailto:ugyfelszolgalat@itm.gov.hu)

Website: <https://www.kormany.hu/hu/innovacios-es-technologiai-miniszterium>

## **Definitions**

The following terms shall be interpreted as per their definitions below for the purposes of this Policy.

**Dataset**: the aggregate of data managed in one record.

**Data processor**: a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

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

**Data controller**: any natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by EU or Member State law, the controller or the specific criteria for its nomination may be provided for by EU or Member State law.

**Data breach**: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

**Recipient**: a natural or legal person, public authority, agency or other body, to which the personal data are disclosed, whether a third party or not.

Public authorities which may receive personal data in the framework of a particular inquiry in accordance with EU or Member State law shall not be regarded as recipients; the processing of data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

**Data subject:** any natural person who can be directly or indirectly identified by any specific personal data. For the purposes of data management under the scope of this Policy, a data subject is

- a. primarily a **User** who is a natural person and who is registered on the Website or a
- b. natural person whose personal data were disclosed by a business participating in the program to the **Contact Person** for a service provided by the Data Controller.

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

**Authority:** the National Authority for Data Protection and Freedom of Information.

**Website:** <https://mmp.ifka.hu/>

**Consent of the data subject:** any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, via a statement or a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

**Public disclosure:** disclosure of data to be to be accessible without limitation.

**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, an identification number, location data, an on-line identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

**Service:** any service available on the Website. This Policy is not applicable to any other services accessible on any other websites, even if they are related to the Future Hungarian Multinationals.

### **Principles relating to processing of personal data**

Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject ("lawfulness, fairness and transparency"). Personal data shall be collected for specified, explicit and legitimate purposes, and not further processed in a manner that is incompatible with those purposes ("purpose limitation"). Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("data minimization"); Personal data shall be

accurate and, where necessary, updated; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (“accuracy”). Personal data shall be kept 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 (“storage limitation”); Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures (“integrity and confidentiality”).

The Data Controller is obliged to act in accordance with the requirements of good faith and fairness, and in cooperation with the data subject, if necessary. Rights and obligations shall be exercised and performed in accordance with their purpose.

### **Purpose of data processing**

Data management by the Data Controller and their transfer to data processors, if necessary, serve the following purposes for the Future Hungarian Multinationals:

- a drafting, concluding and performing the agreement to be concluded with the Data Controller, exercising the rights and performing the obligations arising from the agreement after termination of the agreement, especially compensation arising from the agreement;
- b identification of and communication with Users and Contact Persons, as well as identification of services available to them;
- c performance of the Data Controller’s legal obligations and the purposes of its legitimate interests;
- d ensuring the regular flow of business for the services rendered by the Data Controller, as well as the prevention, investigation and detection of any forms of abuse;
- e in case of an express consent to do so, seeking direct contact by the Data Controller for business development or market research purposes (via mail, telephone or any electronic or other forms of communication);
- f providing an interface (storage) for User and Contact Person (comments, etc.);
- g maintaining records, developing statistics and analyses;
- h technical development of the IT system.

### **Data subjects**

Natural persons whose personal data are managed by the Data Controller.

The data subjects of this Policy and the Future Hungarian Multinationals are primarily

- a. the User and
- b. the Contact Person

### **Client**

The Data Controller shall primarily manage the data of **Clients who are economic corporations that interact with it in a client relationship, have applied to the Program or are users of its services offered on a contractual basis.** Therefore, this Policy does not apply to Clients, since the management of economic corporations' data is not governed by the data processing and data protection regulations applicable to personal data privacy.

## **User**

The Data Controller manages the personal data of natural persons it interacts with in relation to the Future Hungarian Multinationals, as a result of their own interest and initiative, or for an economic corporation to participate in the Future Hungarian Multinationals as a Client upon the referral of an existing User. The contract allowing participation in the Future Hungarian Multinationals is concluded between IFKA and the Client. Conclusion or absence of a client agreement does not affect the relationship between the User and the Data Controller or the Data Controller's data processing obligations or the User's relevant rights.

## **Contact Person**

The Data Controller shall manage the personal data of natural persons registered by a Client economic corporation as its legal representative (executive officer, general manager, managing director, etc.) or upon registration in the Client Profile data by its formally authorized representative during or subsequent to its participation in the Future Hungarian Multinationals. If the Client fails to name a specific individual as contact person, IFKA shall communicate with the Client using the contact details appearing in the business registers (official seat, mailing address, email address).

The data of Users and Contact Persons are managed in separate databases. With the necessary statements made by an authorized person, a given natural person may be registered in both databases; however, a change in the data recorded in one database shall not automatically result in a change in the data of the other database.

## **Lawfulness of processing under this Policy**

### **Legal obligation**

Processing is necessary for compliance with a legal obligation to which the controller is subject. If processing of personal data is rendered mandatory by law (e.g., Act C of 2000 on accounting,) the processing of such data is binding. Data processing to the extent and within the scope required for compliance with a legal obligation does not require the data subject's consent.

### **Performance of a contract**

Data processing is necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into a contract.

### **Legitimate or vital interests**

The Data Controller shall process the data subject's personal data necessary for the purposes of the legitimate interests pursued by the Data Controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. The Data Controller shall also process the data subject's personal data if processing is necessary in order to protect the vital interests of the data subject or of another natural person.

### **Data subject consent**

The Data Controller may also process the data subject's personal data if the data subject had given prior consent to the processing of his or her personal data for one or more specific purposes. Consent of the Data Subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. Consent may not be based on failure to act, it must require active contribution. Information regarding a request for consent shall be deemed adequate if it is presented in a manner which is in an intelligible and easily accessible form, using clear and plain language and provides sufficient information regarding all significant elements of data processing. In the case of consent-based data processing, the data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. If the intended transaction cannot be concluded without the given data processing, the lack of consent shall prevent the transaction from being completed.

The Data Controller shall define the scope of data to be processed for its various purposes in relation to the GINOP-1.1.4-16-2017-00001 Future Hungarian Multinationals on its website at <https://mmp.ifka.hu/>, and provide additional information on the duration of data storage, the purpose of data processing, the transfer of data, data processors engaged in the process and all fundamental facts and circumstances which enable the data subject to make a voluntary and reasoned decision on whether or not to consent to the data processing at [https://mmp.ifka.hu/mmp2teszt/medias/12/adatkezelesi\\_tajekoztato\\_rendezyenyhez.pdf](https://mmp.ifka.hu/mmp2teszt/medias/12/adatkezelesi_tajekoztato_rendezyenyhez.pdf).

### **Lawful basis when processing the personal data of a third party (Contact Person)**

In the event that the Client - its legal or authorized representative - registers personal data of a third person (Contact Person) on the Website, such representative of the Client is obliged to duly obtain the Contact Person's consent to the processing of his or her personal data with regard to the data content required by the Future Hungarian Multinationals. The Data Controller shall have no liability in case the person registering the data had failed to duly inform the Contact Person or obtain his or her consent. Such a circumstance shall have no bearing on the Contact Person's data subject rights and obligations.

## **Data processing activities**

### **Client data processing**

Participation in the Future Hungarian Multinationals is open to businesses (Clients) that meet the qualification requirements set forth in Section (1) of §3 of Act XXXIV of 2004 on small and medium-sized enterprises and aid for their development (hereinafter referred to as: the **SME Act**). As part of the registration process, the Client shall record the corporate data also found in the business registers into the Data Controller's system, including the name of its legal representative (general manager, managing director), official seat (address) and the email address that the business registers record as the address for service or contact email address.

The content of such data may be modified or erased in compliance with the Registration Act when and if the company's data, as recorded in the business registers, are modified. Corporate data processing is not governed by either the GDPR or the Information Act.

### **Processing the personal data of the Client's legal or authorized representative**

Upon making a binding client declaration of legal significance (conclusion of a contract), the Data Controller shall record the personal data of the natural person authorized to make such declarations and shall manage those data for the duration prescribed by law depending on the contents of the declaration, but for at least one year after the statute of limitations and, in case of legal proceedings in progress, until a final ruling on the case. Within the scope of such data management - if it is justified in terms of the legal declaration or prescribed by the relevant regulations of the Future Hungarian Multinationals- the Data Controller may make a copy of the documents containing the personal identification data of the natural person authorized to make such declarations in the Clients name and may also verify the contents of such documents at the National Office for Personal Data and Address Registration.

### **Processing of Contact Person's personal data**

The Data Controller shall manage certain personal data (name, position, phone number, email address) of the Contact Person designated by the Client to act as contact person as long as it manages the Client's other data, unless otherwise stipulated by the Client or the Contact Person. The Data Controller 's primary channel of communication with the Client shall be the Client's legal or authorized representative.

### **Processing of user data**

All natural persons may register on the Future Hungarian Multinationals Website as Users with their name, email address and phone number. The Data Controller shall modify or erase the User's data as per the User's instructions. Unless the User otherwise prescribes, the Data Controller shall manage the User's data during the entire operation of the Future Hungarian Multinationals, shall regularly inform the User of the purposes for which its data is used, along with the events and achievements of the programs (newsletter).

## **General data processing provisions**



The Data Controller shall always ensure that the data it manages is accessible only to the extent necessary, and only to persons to whom those data are essential in performing their duties.

Data processing always records the time of logging into and out of the Website, the used IP address and the user name and password of the user active on the site in the so-called event (log) file, which the Data Controller shall store for at least 6 years from the date of the event for reasons of legitimate interests, and for at least until one year after the statute of limitations and, in case of legal proceedings in progress, until a final ruling on the case, without the option to modify or erase upon request.

The cookies used upon visiting the Website are detailed in the Website's Cookie Policy.

Upon request, modification or erasure of data that can be performed shall be completed by the Data Controller within no more than 25 days from receiving the lawful request, if it cannot be done by the data subject on his or her profile page.

### **Data transfer**

The Data Controller may transfer the personal data of the Client's legal or authorized representative, or those of its Contact Person to data processors stipulated in this Policy for specified purposes, especially for the purpose of compliance with regulatory requirements or performing its contractual obligations arising from the Future Hungarian Multinationals, as well as to designated bodies or organizations required by law or relevant contract.

With due regard for legitimate interests, the Data Controller may transfer the User's name, email address and telephone number, name of legal or authorized representative, the name of Contact Person, name of his or her workplace, position, email address and phone number to organizations that wish to contact such persons with directed offers and proposals, professional and other commercial materials which are relevant to the nature of the Future Hungarian Multinationals.

With the exception of statutory data transmission, the Data Controller may only transmit data to third parties with the data subject's prior consent. Consent may be withdrawn at any time; however, withdrawal has no bearing on the lawfulness of data transfers performed prior to the date of withdrawal. The Data Controller shall keep a separate and updated record of data transfers.

### **Data security**

The Data Controller shall ensure the security of personal and other data in its possession. Taking into account the state of the art technology, the costs of implementation and the nature, scope, context and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Data Controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk. To this end, the Data Controller shall implement and continuously operate the necessary technical and organizational measures to safeguard all data stored in electronic or traditional paper format.

It shall also take measures for the pseudonymization and encryption of personal data, the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services. It shall ensure the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident. It shall take steps to ensure that all relevant statutory data security regulations are adhered to. The Data Controller shall take all necessary measures to protect all data from unauthorized access, alteration, transmission, disclosure, deletion or destruction, as well as accidental destruction and damage, and inaccessibility due to changes in the technology used.

Data security also imposes express obligations on the data subjects and Clients, meaning sound administration and the obligation on the part of data subjects and Clients to ensure that identification codes required for their access to the Website are securely stored to deter unauthorized persons from accessing the system and thereby creating unauthorized exposure to data, allowing their modification, erasure, copying, transmission etc. The Data Controller expressly excludes all liability for damages caused by actions or negligence attributable to the intentional or unintentional behaviors of data subjects or Clients.

With respect to its obligation to ensure IT security, the Data Controller shall act with special care regarding:

- a. protection of datasets from viruses and other malicious code, applications,
- b. measures implemented to ensure the ability to restore data sets (regular back-up facilities, the separate and safe handling of back-up files),
- c. deterring unauthorized access (software and hardware safeguards alike).

## **Rights of the data subject and exercising such rights**

### **Right to information in advance**

The data subject is entitled to obtain facts and information pertaining to the data management prior to the commencement of such activity.

### **Information to be provided when personal data are collected from the data subject:**

- a) the identity and the contact details of the controller and, where applicable, of the controller's representative;
- b) the contact details of the data protection officer, where applicable;
- c) the purposes of the processing for which the personal data are intended, as well as the legal basis for the processing;
- d) the legitimate interests of the data controller or the relevant third party;
- e) categories of recipients of the personal data, if any;

The Data Controller shall, at the time when personal data are obtained, provide the data subject with the following additional information necessary to ensure fair and transparent processing:

- a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine the length of such period;
- b) the right to request access to, and rectification or erasure of personal data or restriction of processing concerning the data subject from the controller, and to object to processing, as well as the right to data portability;
- c) where processing is based on data subject consent, the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
- d) the right to lodge a complaint with a supervisory authority;
- e) whether obtaining personal data is based on statutory or contractual obligation, or is a pre-condition to concluding a contract, or the data subject is obliged to share his or her personal data, and what possible consequences may result from failure to provide such data;
- f) the existence of automated decision-making, including profiling, and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

#### **Information to be provided when personal data are not collected from the data subject**

- a) the identity and the contact details of the controller and, where applicable, of the controller's representative;
- b) the contact details of the data protection officer, where applicable;
- c) the purposes of the processing for which the personal data are intended, as well as the legal basis for the processing;
- d) relevant personal data categories;
- e) recipients or categories of recipients of the personal data, if any;
- f) where applicable, information regarding the transmission of personal data to third countries or international organizations.

#### **Right of access by the data subject**

The data subject is entitled to receive information from the Data Controller on whether his or her personal data are being processed, and if such data processing is occurring, whether he or she has the right to access his or her personal data, and information regarding the processing thereof:

- a) purposes of data processing;
- b) relevant personal data categories;

c) categories of recipients that have or will receive the personal data, including recipients or international organizations located in third countries;

d) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

e) the existence of the right to request access to and rectification or erasure of personal data from the Data Controller, or restriction of processing concerning the data subject, and to object to processing;

f) the right to lodge a complaint with a supervisory authority;

g) where data were obtained from sources other than the data subject, all information available on the source; the existence of automated decision-making, including profiling, and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

The Data Controller shall provide the data subject access to a copy of the personal data that is the subject of processing. The Data Controller may charge a fee commensurate to the extra administrative expenses generated if additional copies are requested by the data subject. If the data subject had submitted his or her request electronically, the response to his or her request shall also be given via a widely used electronic means, unless otherwise requested by the data subject. The right to request a copy may not have any adverse effect on the rights and freedoms of others.

### **Right to erasure (“the right to be forgotten”)**

The data subject has the right to request that the Data Controller erase his or her personal data without undue delay and the Data Controller is obliged to erase the data subject’s personal data without undue delay if any of the following circumstances hold true:

a) the personal data are no longer necessary for the purpose for which they were collected, or they have been otherwise processed;

b) the data subject withdraws his or her consent serving as legal basis for the data processing, and the data processing has no other lawful basis;

c) the individual objects to the processing of his or her data, and there is no overriding legitimate interest to continue this processing, or the data subject objects to processing his or her personal data for direct marketing purposes;

d) the personal data have been unlawfully processed;

e) the personal data must be erased for the Data Controller to comply with a legal obligation prescribed by EU or national legal regulations;

f) the personal data have been collected to offer information society services.

### **Communication of a personal data breach to the data subject**

When the personal data breach is likely to result in a high risk to the rights and freedoms of

natural persons, the Data Controller shall communicate the personal data breach to the data subject without undue delay.

### **Right to rectification**

The data subject shall have the right to obtain the rectification of their inaccurate personal data from the Data Controller without undue delay. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement. The data subject and the Client may modify the data registered in the profile menu at any time, and may also exercise this right at any time in writing via the postal or email address designated on the Website.

Modification shall only result in the overwriting of data (that is the erasure of previous data), if there are no legal barriers to erasure. In all other instances, modification shall result in the recording of new data with a time stamp indicating the time of change, while the previous data also remain in processing. Unless otherwise expressly prescribed by the interested parties, transactions in progress at the time of modification shall be completed as per the (previous) data provided upon initiating the transaction.

The Data Controller shall perform modification requests received within no more than 25 days from their receipt.

### **Right to restrict processing**

The data subject shall have the right to obtain restriction of processing from the Data Controller, where one of the following applies:

- a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;
- b) the processing is unlawful, and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
- c) the Data Controller no longer requires the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defense of legal claims; or
- d) the data subject claims to have objected to the processing of his or her data; in such cases, data processing shall be restricted for the period until which it can be ascertained whether the Data Controller's legitimate grounds override the data subject's legitimate grounds.

### **Right to data portability**

The data subject shall have the right to receive his or her personal data, which he or she has provided to the Data Controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another data controller without hindrance from the controller to which the personal data had been provided, where:

- a) the processing is based on consent or on a contract; and

b) the processing is carried out by automated means.

As part of exercising his or her right to portability of personal data, the data subject may request that the data controllers directly transfer data to one another, if technically possible.

### **Legal remedies**

The primary, fastest and most reliable tool to remedy any issues arising between data subjects and the Data Controller is direct conciliation between the parties, or with the assistance of a moderator, if necessary. Thus, we encourage all data subjects to contact any of the Data Controllers indicated at the beginning of the Policy directly and with confidence if they have any questions, observations, problematic issues, or have experienced any deficiencies, or to indicate such issues via the contact channels indicated on the Data Controllers' own websites.

In the event that such conciliation appears to be impossible due to the nature or conditions of a situation, the data subject may initiate National Authority for Data Protection and Freedom of Information (hereinafter referred to as: **Authority**) proceedings if he or she detects a breach of conduct by the Data Controller. We hereby emphasize that the Authority also recommends that when the problem first arises, the data subject should turn directly to the Data Controller to seek an amicable solution, which is, of course, not a mandatory procedure. The Authority's website is available at <https://www.naih.hu>, via email at [ugyfelszolgalat@naih.hu](mailto:ugyfelszolgalat@naih.hu), or by post at 1530 Budapest, Pf.: 5.

The data subject may file court proceedings in the event of infringement of his or her rights. The suit shall be judged by the courts. The suit shall be filed at the court with jurisdiction at the data subject's place of residence or permanent address (depending on the data subject's preference).

### **Contact details for data processing and data protection issues regarding the Future Hungarian Multinationals:**

#### **IFKA Public Benefit Nonprofit Ltd.**

Official Seat: 1062 Budapest, Andrásy út 100.

Phone Number: +36 (1) 213 2213

Email address: [info@ifka.hu](mailto:info@ifka.hu)