

The following Privacy Notice has been adopted during the December 2020 session by the Board of Trustees of ICDT.

7th December 2020, Budapest

György Surányi

Chairman of the Board of Trustees

PRIVACY NOTICE AND INFORMATION ON THE PROCESSING OF PERSONAL DATA

The International Center for Development and Democratic Transition (hereafter referred to as: ICDT), in compliance with the Regulation No 2016/679 of the European Parliament and of the Council (hereafter referred to as: GDPR) adopted the following Privacy Notice and Information on the Processing of Personal Data:

1. DESCRIPTION OF THE DATA CONTROLLER

ICDT is regarded as data controller.

Information on ICDT:

Name: International Center for Development and Democratic Transition

Head office: 1022 Budapest, Bogár utca 29/C

Tax number: 18907373-1-41

Public-benefit category: Non-public-benefit

Registration number: 01-01-0012474

Number of the order of the registration to the Court: 0100/Pk.60321/2017

Phone number: +36306404010

E-mail: info@icdtfoundation.hu

Web: <https://www.icdtfoundation.com>

Representatives and the Members of the Board of Trustees:

1. György Surányi, Chairman
2. István Gyarmati, Director General
3. László Várkonyi (Founder)

2. DEFINITION OF TERMS (In compliance with the relevant provisions of the GDPR)

- a) **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 online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
- b) **Processing data:** any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction
- c) **Restriction of processing:** the marking of stored personal data with the aim of limiting their processing in the future
- d) **Profiling:** any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements
- e) **Pseudonymisation:** the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person
- f) **Filing system:** any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis
- g) **Controller:** a 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 Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law
- h) **Processor:** a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller
- i) **Recipient:** a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. ²However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing
- j) **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 authorised to process personal data
- k) **Consent of the data subject:** 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

- l) **Personal data breach:** a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed
- m) **Genetic data:** personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question
- n) **Biometric data:** personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data
- o) **Data concerning health:** personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status

3. DESCRIPTION OF THE DATA PROCESSOR

ICDT

Operation and maintenance of the website: ICDT

IT solutions: ICDT

Accounting and payroll services:

Name of the company: MÉHÉSZ TAX CONSULT KFT.

Head office: 1113 Budapest, Karolina út 16.

Registration number: 01-09-709130

Tax number: 12902624-2-43

Activity: accounting and payroll services, preparation of tax returns

4. GENERAL RULES OF DATA CONTROL

- a, Personal data will be available to authorized employees of ICDT, and to individuals and organizations working for ICDT on the basis of a service contract, to an extent needed for the implementation of their tasks.
- b, The data controlling activity considered in this privacy notice refers to the personal data of natural persons, and besides the natural persons subject to data control, it concerns ICDT.
- c, The Director General of ICDT shall ensure that all employees of ICDT follow the provisions of the GDPR, and the rules of this privacy notice.
- d, Personal data handled by ICDT is stored at its head office, in the form of electronic files in a database. In some cases data is stored in paper-based form, in compliance with the statutory requirements regarding data security. ICDT handles the data through non-automated decisions.
- e, The Director General of ICDT shall ensure that the natural person subject to data control will be informed about the statutory basis, or contractual obligation requiring the natural person to provide personal data, as well as informing the natural person whether or not providing personal data is an obligatory prerequisite of contracting. The Director General shall also ensure that the natural person subject to data control will be informed if providing

personal data is obligatory, and about the possible consequences in case the natural person would not provide personal data.

The Purpose of data control:

Data control is a key element of the operations conducted by ICDT, as it contributes to the successful organization of workshops, conferences, and other events including professional activities.

Time frame of data control:

ICDT continues data control until the retraction of the natural person's consent regarding the use of their personal data. Consent can be retracted at any time by sending an email to info@icdtfoundation.hu, expressing the natural person's request to retract their consent regarding data control.

Source of the data:

Sources, which arise during the operations of ICDT. The source of data could be: workshops, conferences, and other events including professional activities.

5. THE DATA CONTROLLING ACTIVITIES OF ICDT

- Relevant data on the projects of ICDT
- Database of the volunteers at ICDT
- List of press relations and connections
- List of donors
- Data control required for the fulfillment of contracts
- Data control connected to employment
- Personal data of executive officers at ICDT
- Personal data of the members of the Board of Advisors at ICDT
- Data control required for the fulfillment of accounting obligations
- Data control connected to the fulfillment of tax-, and other contributions

6. THE LEGAL BASIS OF DATA CONTROL

a, Consent of the person (subject to data control)

The legality of data controlling activities shall be based upon the consent of the subject to data control, or upon any other statutory basis.

7. THE RIGHTS OF THE PERSON BEING SUBJECT TO DATA CONTROL

a, **The person being subject to data control is informed about their rights by ICDT**

The person concerned has a right to:

1. be fully informed before the start of the data control,

2. receive feedback from the data controller whether or not the data control is being conducted at the moment, and if yes, the person concerned is entitled to be informed about personal data and certain information,
3. require the correction or deletion of data, and to be informed once the request is fulfilled,
4. require the limitation of data control, and to be informed once the request is fulfilled,
5. data portability,
6. objection, if their personal data is being used for general interest, or treated on the basis of the data controller's legitimate interest,
7. be informed about the data security incident,
8. retract their consent at any time,
9. lodge a complaint to the supervisory authority

b, Providing detailed information on the rights of the person subject to data control

The right to information

- (1) The person concerned is entitled to receive information regarding data control before the mentioned activity starts

c, Limitations

- (1) The European Union or Member State law applicable on the person being the subject to data control may limit certain provisions in accordance with relevant rights and obligations, in case of the limitation being in compliance with fundamental rights and freedoms and being proportional and required to protect the following points within a democratic society:
 1. national security;
 2. defense and security;
 3. public security;
 4. prevention, investigation or detection of crime, prosecution, or the implementation of crime sanctions, including the prevention of-, and protection from any danger threatening public safety;
 5. Important objectives with general public interest of the European Union or the Member States of the European Union, particularly the economic or monetary objectives of high importance, including questions regarding monetary-, and fiscal policy and taxation, public health and social safety;
 6. Judicial independence and the protection of court proceedings;
 7. The prevention, investigation and detection of ethical wrongdoings regarding regulated professions; and the conduction of any investigation connected to such a case;
 8. Supervision, examination of regulatory activities regarding the implementation of tasks of public authority;
 9. The protection of the person concerned, or the protection of the rights and freedoms of others;
 10. Fulfillment of civil-law demands.

8. PROCEDURE IN CASE OF THE REQUEST OF THE DATA SUBJECT

- (1) ICDD helps the person concerned in exercising their rights, and must not refuse the fulfillment of their rights stated in this privacy notice unless it is proved that ICDD is not in the position to identify the person in question.
- (2) ICDD informs the person concerned about the measures taken as the consequence of the request within one month latest, and without any unjustified delay. If it is required, considering the complexity and number of requests, this deadline can be prolonged by an additional two months. The data controller informs the person concerned within one month after receiving the request about the reasons leading to the delay.
- (3) If the person concerned applied the request in electronic format, ICDD shall inform the person in question by electronic means, unless it is requested otherwise.
- (4) In case of ICDD not taking measures on the basis of the request of the person concerned, ICDD shall provide information on the reasons behind the absence of such measures without any delay, and within one month from receiving the request.
- (5) ICDD takes the relevant measures and provides information towards the person applying the request free of charge, regarding the following topics: feedback on the data control of personal data, providing access to the data being the subject of data control, correction, completion and deletion of data, limitation of data control, data portability, objection against the data control and providing information on the data security incident.
- (6) The data controller shall bear the burden of proving the possibly unfounded and exaggerating nature of the request
- (7) In case the data controller has a valid ground to be concerned about the identity of the natural person applying the request based on Article 15-21 of the Regulation, the data controller is entitled to request further information in order to verify the natural person's identity, as long as it complies with Article 11 of the Regulation.

9. PROCEDURE TO BE APPLIED IN CASE OF A DATA SECURITY INCIDENT

- (1) Within the meaning of the Regulation, a data security incident is referred to as damage to security, which results in the accidental or unlawful destruction, loss, alteration of-, and providing unauthorized disclosure or access to stored or controlled data in any other way.
- (2) The loss or theft of an electronic device (laptop, mobile phone) is considered as a data security incident. Also, the loss or rendering inaccessible the code required to decrypt data encrypted by the data controller, a ransomware attack that results in making data controlled by the data controller inaccessible until the ransom fees are paid, a cyber-attack against the IT system, or an accidentally sent e-mail including personal data to a false address, or the disclosure of the list of addresses etc.
- (3) In case of the detection of an incident, the representative of ICDD conducts an immediate investigation in order to identify the data security incident, and to examine the possible consequences of the incident. To avoid damages, required steps shall be taken.
- (4) Without any unjustified delay, and if possible, within 72 hours from the incident's detection, the data security incident shall be reported to the relevant supervisory authorities, unless the incident most likely does not lead to any risks in connection with

the rights and freedoms of natural persons. If reporting the incident is not completed within 72 hours, reasons validating the delay shall be attached to the report.

- (5) The data processor shall, without any unjustified delay, report the data security incident to the data controller immediately.

10. REGULATIONS ON DATA SECURITY

Principles of the implementation of data security:

- ICDT only controls personal data accordingly to activities mentioned in this Privacy Notice, and according to the purpose of data control
- ICDT is in charge for data security, and is responsible to do the outmost, including technical and organizational steps, in order to ensure the protection of laws on data security, and regulations on secrecy and data security.
- ICDT allows access to personal data to employees, who physically or verbally signed a Declaration of confidentiality, therefore assured to comply with data security regulations.

11. RULES ON DATA PROCESSING

- The rights and obligations of the data processor regarding the data control of personal data are rooted in relevant laws and defined by the data controller, in compliance with laws on data control.
- ICDT declares, that the data processor is not entitled to make decisions regarding data control, and the accessed personal data can only be handled according to the guidelines of the data controller. The data processor is not entitled to process data for own personal purposes, and is obliged to store and preserve data according to the guidelines of the data controller.
- ICDT is responsible for the legality of the data controlling instructions given to the data processor.
- ICDT bears the burden of providing information for the persons concerned about the identity of the data processor, and the place of data procession.
- ICDT does not entitle the data processor to use the service of any further data processor.