PRIVACY POLICY

1. The aim and scope of the document/statement

1.1. The general purpose of the Privacy Policy (hereinafter referred to as the "Policy") is to make public the policies, principles, provisions and instructions of the Central European Service for Cross-border Initiatives (officially abbreviated as CESCI) (registered seat: 1067 Budapest, Teréz krt. 13.), (hereinafter referred to as the "Controller"), regarding data protection and management.

1.2. Regarding the role of the Controller, the scope of the Policy covers the processing of personal data of the users obtained by the Controller.

1.3. The scope of the Policy does not cover the data processing activities of other organisations and service providers whose privacy policies are not considered binding by the Controller, however, their websites are directly accessible via links on the Controller's website. The activities of such organisations are determined by the rules, set out in their own privacy policies. The Controller does not assume any responsibility for the lawfulness of the data processing of these organisations.

1.4. The Controller ensures that the User is informed electronically or in person of the content of this Policy, accepts it and is able to exercise their rights in accordance with point 13 before using its services.

1.5. Legislation taken into account in the preparation of the Policy, in particular:

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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 (General Data Protection Regulation) (hereinafter referred to as Regulation)
- Act V of 2013 on the Civil Code (hereinafter referred to as Civil Code)
- Act CXII of 2011 on the Right of Informational Self-Determination and Freedom of Information (hereinafter referred to as Privacy Act)
- Act C of 2003 on electronic communications (in relation to cookies)
- Act C of 2000 on Accounting (in relation to accounting documents).

2. Definition of terms frequently used in the Guide/policy/document

Under Article 4 of the Regulation

2.1. personal data: any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is the 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 a natural person;

2.2. data 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, storage, adaptation or alteration, retrieval, consultation, use, transmission of disclosures, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

2.3. controller: the natural or legal person, public authority, agency or any 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;

Key data of the Controller according to the Policy:

Official name: Central European Service for Cross-border Initiatives (Officially abbreviated name: CESCI) (hereinafter referred to as: Controller)

Legal form: association of public utility

Registered seat: 1067 Budapest, Teréz krt. 13.

Office: Budapest, 1137 Budapest XIII., Újpesti rkp. 5. III./12A

Registration number: 01-02-0010819 (Metropolitan Court of Budapest)

Tax number: 18188071-2-42

Main operational objectives: To promote socio-economic cooperation between the Hungarian communities, territorial units outside our borders and Hungary in order to ensure the continuous and adequate performance of the public tasks of the state arising from its responsibility for the fate of the Hungarians living outside our borders, as stated in Article D) of the Foundation of the Fundamental Law of Hungary, as well as to assist in the performance of the public tasks of the state arising from the creation of a European unity, as stated in Article E) of the Foundation of the Fundamental Law of Hungary, and from the status of the European Union membership, as well as from the institutional relations;

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

2.5. 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;

2.6. 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;

Pursuant to Section 3 of the Privacy Act

2.7. data subject: any natural person identified or directly or indirectly identifiable by reference to specific personal data;

2.8. data set: all data processed in a single file;

2.9. disclosure: ensuring open access to the data;

2.10. data transfer: ensuring access to the data for a specified third party;

2.11. data deletion: making data unrecognisable in a way that it can never be restored again;

2.12. data destruction: complete physical destruction of the data carrier recording the data;

Other related terms

2.13. social media platforms: media tools used or operated by the Controller (website, Facebook page, etc.), collectively;

2.14. publication: any online or offline publications produced by the Controller as part of its activities or otherwise related to it;

2.15. service: a set of services provided in accordance with the objectives of the Controller, in particular

- professional (excluding independent legal activities operating under legal conditions) and other legal services (in particular those related to strategy development, situation analysis, project development, calls);
- organised events (workshops, trainings, educational courses, events, conferences, community discussions, community forums, etc.),
- displayed vacancies.

2.16. user: the natural person concerned who uses or registers to use the services referred to in point 2.15 and thereby provides one or more of the personal data listed in point 3;

2.17. employee: a natural person employed by or otherwise contracted to the Controller;

2.18. potential employee: a natural person who applies for one of the job vacancies advertised by the Controller (job, scholarship or volunteer work);

2.19. automated data set: a set of data to be processed automatically;

2.20. system: the entirety of the technical solutions that enable the Controller's services available on the Internet.

3. Purpose and legal basis of data processing

3.1. The purpose of data processing is:

a) to provide high quality online and offline services related to the operation of the Controller, tailored to user needs;

b) to identify the User and the services he/she can use, and to provide storage space for the content generated by the User (e.g. comments, forums);

c) to provide information on the protection of the rights and the enforcement of the legitimate interests of the Controller, the User and third parties;

d) to carry out the Controller's project implementation activities by providing the required data;

e) to keep regular records of the Controller's employees and to recruit and select potential employees;

f) to produce other statistics and analyses related to the activities of the Controller;

g) to send out marketing materials;

h) to technically improve the IT system of the Controller;

i) to facilitate the conclusion and performance of contracts within the scope of the Controller's activities;

j) to maintain contact in relation to the activities of the Controller.

3.2. The Controller shall not use the personal data provided and processed for purposes other than those indicated.

4. Principles of data processing

4.1. The Controller shall process the User's personal data in accordance with the applicable law and on the basis of the User's explicit consent in accordance with the purposes set out in the Policy, to a degree proportionate to the purpose of the data processing.

4.2. If the Controller intends to use the processed personal data for purposes other than those for which they were originally collected, the Controller may do so only with the prior explicit consent of the User, unless otherwise provided.

4.3. The User shall be given the opportunity to make a decision on the processing of his/her personal data, either in person or by written declaration, taking into account the provisions of point 11.

4.4. The Controller processes personal data in accordance with the principles of good faith, fairness and transparency and in accordance with the applicable law and the provisions of this Policy.

4.5. The Controller is not obliged to verify the accuracy of the personal data provided. The responsibility for the authenticity of the personal data lies with the User who provided them.

4.6. According to the Civil Code, the Controller may process the personal data of a natural person who is a minor only with the consent of the legal representative. In the absence of a declaration of consent, the Controller shall not process such data, with the exception of personal data automatically collected when using the website service.

4.7. The Controller shall notify the User of the rectification, restriction or deletion of his/her processed personal data, as well as anyone who previously received the personal data for processing. Notification is not required if, with regard to the purposes of the processing, it is unlikely to undermine the legitimate interests of the data subjects.

4.8. The Controller shall take all necessary technical and procedural measures to ensure the security of the personal data processed and to prevent their accidental loss, destruction, unauthorised access, use, alteration and disclosure.

4.9. No automated decision-making (in individual/specific cases, including profiling) will take place in relation to the Controller.

5. The activities of each controller and related personal data

5.1. The Controller processes the following personal data of the User when using its services: name, place of residence, place of stay, landline and mobile telephone numbers, e-mail address, facial image, voice recording, workplace, position/job title, language spoken, education, age, as well as other personal data provided by the User.

5.2. The Controller may also process other personal data of the User, in addition to those described in section 5.1, in relation to speakers and participants of events organised by the Controller, in the course of its newsletter service and its

activities related to questionnaires, in particular: the name of the organisation associated with the User, the interests of the User.

5.3. In the context of its contracts, the Controller may, in addition to the information referred to in points 5.1 and 5.2, process the following personal data of the contracting User:

- legal or authorized representative and contractual contact person of the contracting User;
- personal data relating to the billing name and address provided by the User, as well as personal data relating to the service to be purchased and the payment method chosen.

5.4. The Controller's processing of data at the workplace is provided for in Section 9.

5.5. The Controller may process demographic data by using a cookie (i.e. data packet) based on any of the personal data in 5.1 and/or 5.2, as well as habits and preferences based on browsing history.

The cookie provides personalised services on the specific websites and enhances the user experience. The Controller will inform the User in advance of its use, and the User will allow or restrict the use of the cookie by deleting it from his/her computer or disabling it in his/her browser.

5.6. During the use of the services of the Controller, as a result of the technical processes of the system, certain personal data of the User may be automatically recorded. Such data may include, for instance, the User's IP address, the type of operating system and browser program, the data of the websites from which the User has accessed or visited the Controller's website, as well as the time and duration of the visits. The data recorded will be logged in the system, without any special declaration or action by the User, when logging in or out of the system. Only the Controller has access to the recorded data.

5.7. The Controller may record the User's IP address, notwithstanding the provisions of Section 5.6, on the basis of legitimate interest or in order to ensure the lawful provision of the service (e.g. to filter out illegal content) without the User's separate consent.

6. Duration of data processing

6.1. Unless otherwise provided by law, the processing of personal data provided by the User in connection with the services provided by the Controller shall continue until the User unsubscribes from the service, otherwise requests the deletion of his/her personal data or their retention, or until the Controller has a legitimate interest in processing the personal data.

6.2. The User's right to use the service shall not be affected by the User's request to cease data processing without unsubscribing from the service, however, the User may not be able to use or fully use certain services of the Controller without his/her personal data.

6.3. The processing time limit for the data automatically recorded by the service provider is governed by the data protection provisions of the respective service provider and the applicable legislation. In this case, the Controller will also endeavour to ensure that the recorded data cannot be linked to other personal data of the User, apart from the exceptions mentioned by law.

6.4. The Controller shall periodically back up the data stored in its IT system during the period of data processing in order to prepare for emergency situations (security purpose) and to guarantee the integrity of the data (evidence purpose), which may also affect the personal data of individual Users and may affect the period of processing thereof.

7. Data processing

7.1. The Controller does not process any personally identifiable data.

7.2. The Controller's system may perform data processing and statistical aggregation on the activity of Users, but this may not be linked in a personally identifiable manner with other personal data provided by the Users, nor with user data generated by other data controllers or data processors.

8. Transfer of data

8.1. The Controller is entitled and obliged to send any personal data stored by it to the competent authority or central bodies involved in the implementation of the application, which it is obliged to transmit by law, final decision of a public authority or grant contract. The Controller shall not be held liable for any such transfer or its consequences,

8.2. The Controller is entitled to transfer the personal data to a designated third party, subject to the prior consent of the User. The transfer of the data shall take place under the full responsibility of the User, with the third party's data management provisions applying to the processing of the data transferred.

8.3. The Controller shall keep records for the purposes of verifying the lawfulness of data transfers and providing information to the User, which shall include the date, legal basis and recipient of the transfer of personal data processed by the Controller, the scope of the personal data transferred and other data specified in the legislation requiring data processing.

9. Data processing in relation to the Controller's employees and potential employees and its office audit

9.1. The Controller may process the following personal data about its employees:

- name, birth name, tax identification number, social security number, mother's name, place/date of birth, identity card number, nationality, permanent address/residence, postal address, bank account number, education and educational qualifications and supporting documents, certificate of clean criminal record, data for establishing pension and social security entitlement,
- spouse's name/birth name/tax identification number,
- the name(s)/ place(s)/ date(s)/ tax identification number(s)/ social security number(s)/ mother's name of the child(ren), and
- additional information voluntarily provided by the employee.

9.2. The purpose of the processing of data relating to the employees of the Controller is to fulfil the legal obligations of the Controller.

9.3. The duration of the processing of data relating to the employees of the Controller shall be determined by the applicable legislations and the legitimate interest of the Controller as applied in accordance therewith.

9.4. By submitting the documents, required for his/her application to the Controller, the potential employee consents to the processing of his/her personal data provided during his/her application by the Controller for the purposes of recruitment, selection and, in the case of a successful application, employment.

9.5. The Controller may operate surveillance cameras at the place of work for reasons related to the performance of the employee's contract or for the protection of property. The images from the cameras may be viewed and used by an authorised representative of the Controller or, where applicable, by a representative of the competent authority, in accordance with the regulations. Unused images must be deleted from the system within 72 hours of their creation.

10. Contract-related data processing

10.1. In the course of the Controller's contracting activities, this policy shall be deemed to be a contractual term that is part of the contract but physically separate from it.

10.2. By signing the contract with the Controller, the party entering into the contract acknowledges that he/she has carefully read and understood the contents of the Policy, has accepted it as the Controller's legally required data protection

measures and has expressly consented to the processing of its personal data by the Controller.

10.3. The provisions of the Civil Code in force shall apply to the enforcement of legal claims arising from contracts with regard to the duration of data processing.

11. Rights and obligations of the User

11.1. Within the scope of his/her rights, the User may request in a verifiable manner that the Controller inform him/her whether the Controller processes any of his/her personal data and, if so, provide access to the electronic and paper records and project documents of the Controller related to such data, if so requested.

11.2. In addition to the personal data processed by the Controller, the User's request for information may include the source of the personal data, the purpose, legal basis and duration of the processing and transfer, the data of any data processors, service providers and other activities related to the processing.

11.3. The User may request the modification of his/her personal data by the Controller in a verifiable manner. Once the request becomes fulfilled, the modified data (except for data changes requiring further modification) can no longer be restored.

11.4. The User may also request the erasure of his/her personal data by the Controller in a verifiable manner. Deletion may be refused, in case:

- the request infringes the exercise of the right to freedom of expression and information;
- further processing of the personal data requested to be deleted is authorised by legislation;
- it prevents the enforcement or defence of legal claims.

The Controller shall inform the User of the refusal of the deletion request, stating the reason. Once the request for erasure of personal data becomes fulfilled, the previously erased data can no longer be restored.

The procedure for erasure of personal data must be clear and verifiable.

11.5. The User may request in a verifiable manner that the Controller restricts the processing of his or her personal data, in case:

- *he/she contests the accuracy of the personal data processed*: this way, the limitation applies for the period of time during which the data are checked and, where necessary, rectified;
- *the processing is unlawful*, but the User objects to the deletion of the personal data in question and requests only the restriction of their use;

- *the purpose of the processing has been achieved*, but the User requests further processing of his or her personal data by the Controller in order to assert or defend legal claims.

11.6. The User may object to the processing of his/her personal data, in case:

- the processing of the User's personal data is necessary solely for the purposes of the *legitimate interests pursued by the Controller or by a third party*, except in cases of mandatory processing;
- the processing is for *direct marketing, public opinion polling or scientific research purposes*;
- other cases specified *by law*.

11.7. The Controller shall be obliged to assess the merits of the User's request for restriction or the lawfulness of the User's objection as soon as possible after the request is submitted, but within 30 days at the latest if the User is prevented from doing so.

11.8. If the User's request or objection is justified, the Controller shall restrict or terminate the processing of the personal data and, if necessary, take measures to ensure that the correct data are recorded, in cooperation with the User, as appropriate; the Controller shall then notify the persons to whom the relevant personal data were previously disclosed of the measures taken.

11.9. The User warrants that the personal data provided or made available to the Controller about another natural person is accurate, that the consent of the natural person concerned has been obtained lawfully for its processing and, where applicable, that the User is acting lawfully on behalf of the other natural person. If the User has unlawfully provided the personal data, the User shall be fully liable in this respect.

12. External providers

12.1. In the course of providing its services, in particular for the operation of its media platforms, the Controller uses or may use an external service provider (hereinafter referred to as "Provider") on a contractual basis.

12.2. The Controller distances himself/ herself from the activities of the contracted service providers, in the course of which they access personal data (e.g. user IP addresses) processed by the Controller through their web applications (e.g. cookies, click measurement) without the specific consent or knowledge of the User or the Controller, and use them to personalise their services and to compile statistics.

12.3. The Controller also distances himself/herself from service providers with which he/she does not have a contractual relationship, but through their technical solutions they may have access to its services and collect data that can be used to identify the User.

12.4. Such service providers may include, but are not limited to: Facebook Ireland Inc., Google LLC, You Tube LLC.

12.5. The personal data stored and processed on the Provider's systems are governed by the privacy policy of the service provider concerned.

12.6. To find out the data management rules applied by such providers, it is recommended to visit the website or customer service of the service provider concerned.

12.7. The web analytics and advertising serving service provider which currently works with the Controller is Google Analytics.

13. Enforcement possibilities

13.1. The User may contact the following employees of the Controller with any questions or comments regarding the personal data processed by the Controller:

Technical matters: Enikő Hüse-Nyerges

Legal issues: dr. Norbert Jankai

Contact

By electronic means: cesci@cesci-net.eu

Personally: at the Headquarters of the Controller:
(1137) Budapest, Újpesti rkp. 5. III./12A

13.2. The User may also contact the National Authority for Data Protection and Freedom of Information directly with a data processing complaint (address: 1125 Budapest, Szilágyi Erzsébet fasor 22/c.; phone: +36-1-391-1400; e-mail: ugyfelszolgalat@naih.hu; website: www.naih.hu).

13.3. In case of violation of the User's rights, he/she may take legal action. The action may also be brought, at the User's option, before the court of the place of residence or domicile.

14. Final provisions

14.1. The Controller reserves the right to unilaterally amend the text of the policy in the light of changes in legislation, the content of new or amended guidelines and other interpretations in accordance with the law.

14.2. In the event of any dispute between the Controller and the User, the terms used in this Policy shall be construed in accordance with the purpose and content of the applicable data protection legislation.

14.3. The policy is available for electronic consultation on the Controller's website and in person at any of its offices.

Budapest, 25 May, 2018.

.....
dr. Tamás Tóth
President