Internal data management and data security policy
Sound-Picture Cultural Association

I. Scope of the Policy

1. The scope of these regulations covers the entire Hang-Kép Cultural Association, all its organizational units and all employees (hereinafter: organization).

II. Purpose of the policy

2. The purpose of the Regulations is to ensure the enforcement of the protection of personal data in accordance with the Basic Law, the implementation of information self-determination, and to determine the data protection and data security rules governing data management in relation to the personal data managed by the organization.

III. Governing legislation

The organisation shall act in accordance with the requirements of the following legislation in its data processing, as set out in these internal rules:

- Regulation (EU) 2016/679 of the European Parliament and of the Council (27 April 2016). European Parliament and Council Regulation (EU) No .../2009 of 27 June 2010 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Regulation (EC) No 95/46/EC (General Data Protection Regulation, hereinafter referred to as "GDPR")
- Act CXII of 2011 on the Right of Informational Self-Determination and Freedom of Information (hereinafter: "the Infotv.")
- Act V of 2013 on the Civil Code (hereinafter referred to as "Civil Code")
- Act I of 2012 on the Labour Code (hereinafter referred to as "Labour Code Act")
- Act No LXXV of 2007 on the Hungarian Chamber of Auditors, Auditing Activities and Public Supervision of Auditors (hereinafter referred to as "Act No LXXV of 2007 on the Hungarian Chamber of Auditors")

IV. Interpretative provisions

4: Concepts defined in the GDPR, of which the following concepts should be highlighted in accordance with the nature of these internal regulations:

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

(c) 'controller' means a 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 the processing are determined by Union or Member State law, the

controller or specific criteria for the designation of the controller may also be determined by Union or Member State law.

(d) 'processor' means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.

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

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

(g) 'filing system' means a set of personal data, structured in any way, whether centralised, decentralised or structured according to functional or geographical criteria, which is accessible on the basis of specified criteria.

(h) 'personal data breach' means 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.

(i) representative: a natural or legal person established or resident in the European Union and designated in writing by the controller or processor pursuant to Article 27 to represent the controller or processor in relation to the obligations incumbent on the controller or processor under this Regulation.

(j) organisation: any natural or legal person, regardless of its legal form, engaged in an economic activity, including partnerships or associations carrying on a regular economic activity.

Additional definitions:

(k) 'data inventory' means a document used to assess the scope and nature of the personal data processed by the controller.

(l) technical and organisational measures: a set of procedures, appropriately defined by the controller, taking into account the nature, scope, context and purposes of the processing and the varying degrees of probability and severity of the risk to the rights and freedoms of natural persons, to ensure and demonstrate that personal data are processed in accordance with the GDPR. These measures shall be reviewed and, where necessary, updated by the controller.

V. Principles of data management

The organisation will process data lawfully and fairly and in a transparent manner for the data subject (lawfulness, fairness and transparency).

The organisation collects personal data only for specified, explicit and legitimate purposes and does not process them in a way incompatible with those purposes (purpose limitation).

7. The organisation will carry out processing that is adequate, relevant and limited to the purpose(s) for which it is intended (data minimisation). Accordingly, the organisation will not collect or store more data than is strictly necessary for the purposes for which it is processed.

8. The organisation shall take all reasonable steps to ensure that personal data which are inaccurate for the purposes of the processing are erased or rectified without undue delay (accuracy).

The organisation shall store the personal data 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, subject to any storage obligations laid down in applicable law (limited storage).

10. the organisation ensures adequate security of personal data, including protection against unauthorised or unlawful processing, accidental loss, destruction or damage to personal data (integrity and confidentiality), by implementing appropriate technical or organisational measures.

11. The organisation is responsible for compliance with the principles detailed above and demonstrates such compliance (accountability). To this end, the organisation shall ensure that the provisions of this internal policy are continuously enforced, that its data management is continuously reviewed and that, where necessary, data management procedures are amended and supplemented. The organisation shall prepare documentation to demonstrate compliance with legal obligations.

VI. Legal bases for data processing

12. The processing of personal data is lawful only if and to the extent that at least one of the legal grounds set out in paragraphs 13 to 18 is fulfilled:

13. the data subject has given his or her consent to the processing of his or her personal data for one or more specific purposes (hereinafter referred to as "processing based on consent").

14. processing is necessary for the performance of a contract to which the data subject is a party or for taking steps at the request of the data subject prior to entering into a contract (hereinafter "processing based on a contract").

15. processing is necessary for compliance with a legal obligation to which the organisation is subject (hereinafter 'processing based on a legal obligation').

16. processing is necessary in order to protect the vital interests of the data subject or of another natural person (hereinafter 'processing based on vital interests').

17. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the body (hereinafter 'processing based on official authority').

18. processing is necessary for the purposes of the legitimate interests pursued by the organisation or a third party, except where those interests are overridden by the interests or fundamental rights and freedoms of the data subject which require the protection of personal data, in particular where the data subject is a child (hereinafter 'processing based on legitimate interests').

19. The legal basis for processing may change during the processing.

VII. Inventory of data assets

20. The organisation shall draw up an inventory of its data assets for the purpose of establishing technical and organisational measures for the processing of data in the course of its activities in accordance with the obligations imposed by the GDPR and the law. The data inventory shall include all the data processed by the organisation.

21: In connection with the organization's data management activities, the following are defined in the data asset inventory:

a) the data subject [e.g. customer, employee, volunteer]
(b) the identity and purpose of the processing [e.g. statutory auditing, workplace processing]
c) the scope of the data processed [e.g. name, address, telephone number, e-mail address, salary]
d) the scope of any special data processed [e.g. trade union membership, health data]
e) the legal basis for processing [e.g. contract, law, legitimate interest]
f) the duration of the processing [e.g. 8 years under the Accounting Act]
(g) who has access to the personal data within the organisation [e.g. auditor, audit assistant, administrative assistant, quality controller]
h) to whom the data may be disclosed [e.g. chamber of commerce, other public authority]
(i) whether the organisation employs a data processor, if so, whom, for what purpose and to what personal data and for how long the personal data may be stored [e.g. payroll, server operator, website operator]

22. In the context of the organisation's data processing activities (if any), the inventory of data assets will specify:

(a) the activity for which the organisation qualifies as a data processor;
(b) who is the controller on whose behalf the processing activity is carried out;
(c) the personal data to which it has access;
(d) for how long it may store the personal data.

VIII. Rights of the data subject and their enforcement

23 The organisation shall provide data subjects with the following rights in accordance with the provisions of the GDPR.

Right to information

24 The right to information is granted to the data subject in relation to all legal bases for processing.

25 The organisation shall provide information to data subjects in a concise, transparent, intelligible and easily accessible form, in clear and plain language.

26 Information shall be provided in writing or by other means, including, where appropriate, by electronic means.

Information at the request of the data subject

27. Information may be provided orally at the request of the data subject, provided that the identity of the data subject has been otherwise verified.

28. The organisation shall inform the data subject of the action taken on the data subject's request concerning other data subjects' rights without undue delay and in any event within 30 days of receipt of the request.

29. Where necessary, taking into account the complexity of the request and the number of requests, the 30-day time limit may be extended by a further 60 days. The organisation shall inform the data subject of the extension, stating the reasons for the delay, within 30 days of receipt of the request. Where the data subject has submitted the request by electronic means, the information shall be provided by electronic means where possible, unless the data subject requests otherwise.

30. The information and action shall be provided free of charge.

31. Where the request of the data subject is manifestly unfounded or excessive, in particular because of its repetitive nature, the organisation shall, subject to the administrative costs of providing the information or information requested or of taking the requested action:
(a) charge a reasonable fee; or
(b) refuse to act on the request.

32. The burden of proving that the request is manifestly unfounded or excessive shall be on the organisation.

Obligatory information

33. Where the organisation has obtained the data directly from the data subject (including in particular clients), the organisation shall in any event provide information on:

(a) the identity and contact details of the organisation's representative, if any;
b) the contact details of the Data Protection Officer, if any;
c) the purposes for which the personal data are intended to be processed and the legal basis for the processing
(d) in the case of processing based on legitimate interests, the legitimate interests of the organisation or third parties;
(e) where applicable, the recipients of the personal data
(f) where applicable, the fact that the organisation intends to transfer the personal data to a third country or an international organisation,
(b) the fact that the data subject is subject to a data protection obligation

34. In addition to the above, at the time of the first acquisition of personal data, the organisation shall inform the data subjects of the following:

a) the duration of the storage of the personal data
(b) the data subject's right to obtain from the organisation access to, rectification of, or, in the case of processing on certain legal bases, erasure or restriction of processing of personal data concerning him or her and, in the case of processing on certain legal bases, to object to the processing of such personal data, and the data subject's right to data portability;
(c) the right to withdraw the processing based on consent at any time, without prejudice to the lawfulness of the processing carried out on the basis of consent prior to its withdrawal;
(d) the right to lodge a complaint with a supervisory authority (National Authority for Data Protection, hereinafter referred to as "the Authority" or "the NDA");
(e) whether the provision of personal data is based on a legal or contractual obligation or is a precondition for the conclusion of a contract, whether the data subject is under an obligation to provide the personal data and the possible consequences of not providing the data.

35. If the organisation intends to further process personal data for a purpose other than that for which they were collected, it shall inform the data subject of that other purpose and of any relevant additional information referred to in point 34 prior to further processing.

36 The organisation may comply with the mandatory information in various ways.

(a) The information referred to in point 34 shall be published by the organisation on its website (under the title "Information Notice on Data Processing") in a manner that is easily accessible and easily available to any person.

b) In addition to or instead of publishing it on the website, the organisation may choose to make the "Information Notice" available as an annex to the contract. In this case, it is sufficient to provide the data subject with the information on the processing of personal data relevant to the data subject concerned. The "Information Notice on Data Management" should not form part of the General Terms and Conditions (GTC).

37. If the organisation has not obtained the data processed in the course of carrying out statutory audit work directly from the data subject, the organisation is not obliged to provide the data subject with the information referred to in points 33 and 34, taking into account the strict confidentiality obligations imposed by the Act on the Statutory Audit of Statutory Audits.

Right of access

38. the data subject has the right of access to all legal bases for data processing.

39: The data subject has the right to receive feedback from the organisation as to whether or not his or her personal data are being processed and, if such processing is taking place, the right to access the personal data and the following information:

a) the purposes of the processing;
(b) the categories of personal data concerned;
(c) the recipients or categories of recipients to whom or with which the personal data have been or will be disclosed
(d) where applicable, the envisaged duration of the storage of the personal data
(e) the data subject's right to obtain from the organisation the rectification of personal data concerning him or her, or, in the case of processing based on certain legal bases, the erasure or restriction of the processing of such data, and, in the case of processing based on certain legal bases, the right to object to the processing of such personal data;
(f) the right to lodge a complaint with a supervisory authority;
(g) where the data have not been collected from the data subject, any available information concerning their source;
(h) the fact of automated decision-making, including profiling, and, at least in these cases, the logic used and clear information on the significance of such processing and its likely consequences for the data subject.

40. The organisation shall provide the data subject with a copy of the personal data that are the subject of the processing.

41. For any additional copies requested by the data subject, the organisation may charge a reasonable fee based on administrative costs, the amount of which will be set out in the organisation's pricing policy, other rules or other document.

Right to rectification

42. The right to rectification is granted to the data subject in respect of all legal bases for processing.

43. The data subject shall have the right to request the completion of incomplete personal data, inter alia, by means of a supplementary declaration.

Right to erasure (right to be forgotten)

44. The right of erasure (right to be forgotten) is not automatic for the data subject in relation to all processing operations related to the legal basis.

45. The organisation shall delete personal data concerning the data subject without undue delay where one of the following grounds applies:

(a) the personal data are no longer necessary for the purposes for which they were collected or otherwise processed;
(b) the data subject withdraws the consent on the basis of which the processing was carried out (in the case of processing based on consent) and there is no other legal basis for the processing;
(c) the data subject objects to the processing and there is no overriding legitimate ground for the processing in the case of legal grounds for processing used in accordance with points 17 and 18 (processing based on public authority or legitimate interest)
(d) the personal data have been unlawfully processed;
(e) the personal data must be erased in order to comply with a legal obligation under Union or Member State law applicable to the organisation;

46. The organisation shall not comply with the data subject's request for erasure where the processing is necessary for compliance with a legal obligation to which the organisation is subject that requires the processing of personal data.

47. For this purpose, the organisation may request the identification data of the contract between the data subject and the organisation (e.g. contract number, date of contract), the identification number of the document issued to the data subject by the organisation, the personal identification data registered about the data subject (the organisation may not, however, request as identification additional data which it does not keep about the data subject).

48. The organisation shall keep a record of the deletion in order to verify that the deletion has taken place. The record shall be signed by the representative of the organisation or by the person(s) authorised to do so by his/her job description. The cancellation report shall contain:

(a) the name of the person concerned
(b) the type of personal data deleted
(c) the date of deletion.

50. The organization informs all those to whom the personal data has been forwarded about the obligation to delete.
The right to restrict data processing
51. The data subject has the right to restriction in relation to all legal grounds for data processing.

52. The organization restricts data processing at the request of the data subject if one of the following is met:

a) the data subject disputes the accuracy of the personal data, in which case the limitation applies to the period that allows the organization to check the accuracy of the personal data;

b) the data management is illegal and the data subject opposes the deletion of the data and instead requests the restriction of their use;

c) the organization no longer needs the personal data for the purpose of data management, but the data subject requires them to present, enforce or defend legal claims; obsession

f) the data subject objected to the data processing in the case of data processing legal bases applied in accordance with points 17 and 18 (data processing based on public authority authority or legitimate interest); in this case, the restriction applies to the period until it is determined whether the legitimate reasons of the organization take precedence over the legitimate reasons of the data subject.

53. If data processing is subject to restrictions on the basis of the previous point, such personal data, with the exception of storage, will only be processed with the consent of the data subject, or for the presentation, enforcement or defense of legal claims, or for the protection of the rights of other natural or legal persons, or the European Union, or can be handled in the important public interest of a member state.

54. The organization informs all those to whom the personal data has been forwarded about the obligation.

Protest

55. The data subject has the right to protest in the case of data processing legal bases based on public authority or legitimate interest.

56. The organization may no longer process personal data in the event of a request for objection from the data subject, unless it proves that the data processing is justified by compelling legitimate reasons that take precedence over the interests, rights and freedoms of the data subject, or which, in order to submit legal claims, are related to its enforcement or protection.

57. If the processing of personal data is carried out for the purpose of obtaining direct business, the data subject has the right to object at any time to the processing of his personal data for this purpose.

58. If the data subject objects to the processing of personal data for the purpose of direct business acquisition, then the personal data may no longer be processed for this purpose.

Right to data portability

59. The data subject has the right to data portability in the case of data processing based on consent or a contract, if the data is processed in an automated manner.

60. The organization ensures that the data subject receives the personal data he/she has provided to the organization in a segmented, widely used, machine-readable format, and that the data subject forwards this data to another data controller.

IX. Registration of data management activities

61. The organization keeps records of data management activities in accordance with the principle of accountability in order to be able to monitor and verify compliance with the GDPR.

62. The organization keeps at least the following records of the data management activities carried out under its responsibility:

a) record of data transfer
b) registration of requests for the enforcement of stakeholder rights and the responses given by the organization
c) registration of official requests and the answers given by the organization
d) registration of requests for termination of data management
e) register of customers
f) registration of inquiries for marketing purposes
g) record of the management of personal data related to the employment relationship
h) recruitment register
i) registration of data protection incidents.

63. The organization keeps records of the data management activities carried out under its responsibility, as specified in point 62, with the following content:

a) the name and contact information of the organization and, if any, the name and contact information of the representative of the organization and the data protection officer;
b) the purposes of data management;
c) description of categories of data subjects and categories of personal data;
d) categories of recipients to whom the personal data is communicated or will be communicated
e) where appropriate, information on the transfer of personal data to a third country or international organization;
f) if possible, the deadlines for erasing the various data categories;
g) if possible, a general description of the technical and organizational measures.

64. If the organization also performs activities as a data processor, the organization keeps records of all categories of data management activities performed on behalf of the organization. This register contains the following information:

a) the name and contact details of the data processor or data processors and their representatives;
b) categories of data management activities performed on behalf of the organization;
c) where appropriate, the transfer of personal data to a third country or international organization.

65. The records are kept by the organization in writing, on paper or in electronic format.

X. Data Security Provisions

66. The organization implements appropriate technical and organizational measures, taking into account the state of science and technology and the costs of implementation, as well as the nature, scope, circumstances and purposes of data management, as well as the varying probability and severity of the risk to the rights and freedoms of natural persons in order to, to guarantee a level of data security commensurate with the degree of risk.

67. Pursuant to the above, the organization is obliged to guarantee the confidentiality, integrity and availability of the data it manages.

68. In order to determine the appropriate level of data security measures, the organization evaluates each data file in its management from the point of view of the need for protection and classifies it into a security level.

69. In order to determine the level of security of individual data management, it is necessary to analyze:

a) the risk and expected damage associated with the unauthorized access, change, deletion of personal data handled, damage to hardware and software devices;
b) whether the damaged data file can be restored, as well as possible costs of restoration, the availability of data sources necessary to reproduce personal data, the possibility of replacing lost data from manual background records;
c) whether, in view of the nature of the processed personal data, it is justified to apply differentiated security standards;
d) other risk elements endangering data security;

70. In order to achieve the security of data management, the organization applies physical, logical and administrative controls together.

71. The organization applies at least the following physical controls:

a) the organization ensures that unauthorized persons cannot enter its building/office by operating an access control system capable of filtering the entry of unauthorized persons [this can be the operation of an electronic access control system; or simple key entry, where the key is only available to those authorized to enter; or any other method that ensures the achievement of the goal]

b) in order to avoid unauthorized access to the data it manages both electronically and on a paper basis, the organization ensures that no unauthorized person can physically access the managed data [closing offices, server rooms; application of monitor foils; placement of monitors in such a way that only authorized persons can see the data on them; only data carriers audited by the organization may be connected to the computers; or anything else, a method that ensures the realization of the goal].

72. The organization applies at least the following logical controls:

a) the organization ensures that the data it manages can only be accessed by those with the appropriate authorization [determination of authorization levels by job; setting access to computer databases according to authorization levels; tying access to the internal computer network to a username and password; or any other method that ensures the achievement of the goal]

73. The organization applies at least the following administrative controls:

a) the organization ensures that any access to personal data can be tracked in documentation [activity logging; logging entry into the building/office (even on paper basis); or any other method that ensures the achievement of the goal]

b) the organization ensures the establishment of a document management procedure so that documents containing personal data received by it in error are filtered out as soon as possible and are known to the narrowest possible circle of personnel it exclusively for this or any other method that ensures the realization of the goal]

XI. Management of data protection incidents

74. In the absence of appropriate and timely measures, a data protection incident may cause physical, financial or non-financial damage to natural persons, including loss of control over their personal data or restriction of their rights, discrimination, identity theft or identity abuse, financial

loss, damage to reputation, damage to the confidential nature of personal data protected by the obligation of professional confidentiality, or other significant economic or social disadvantage affecting the natural persons in question.

75. The organization shall report the data protection incident to the authority without undue delay and, if possible, no later than 72 hours after becoming aware of the data protection incident.

76. The data protection incident does not have to be reported to the authority if the data protection incident is not likely to pose a risk to the rights and freedoms of natural persons.

77. If the notification is not made within 72 hours, the reasons justifying the delay must also be attached.

78. If it is necessary to report the data protection incident to the authorities, then in the report:
a) the nature of the data protection incident must be described, including – if possible – the categories and approximate number of those affected, as well as the categories and approximate number of data affected by the incident;
b) the name and contact details of the data protection officer or other contact person providing additional information must be disclosed;
c) the likely consequences of the data protection incident must be described;
d) the measures taken or planned by the organization to remedy the data protection incident must be described, including, where applicable, measures aimed at mitigating any adverse consequences resulting from the data protection incident.

79. If the data protection incident is likely to involve a high risk for the rights and freedoms of natural persons, the organization shall inform the person concerned about the data protection incident without undue delay.

80. In the information according to point 79, the nature of the data protection incident must be clearly and comprehensibly explained to the data subject, and the following must be communicated:

a) the name and contact details of the data protection officer or other contact person providing additional information;
b) the likely consequences of the data protection incident must be described;
c) the measures taken or planned by the organization to remedy the data protection incident must be described, including, where applicable, measures aimed at mitigating any adverse consequences resulting from the data protection incident.

81. The data subject need not be informed if any of the following conditions are met:

a) the organization has implemented appropriate technical and organizational protection measures and these measures have been applied to the data affected by the data protection incident, in particular those measures - such as the use of encryption - that would be unintelligible to persons not authorized to access personal data they make the data;
b) after the data protection incident, the organization has taken additional measures to ensure that the high risk to the rights and freedoms of the data subject will probably not materialize in the future;
c) providing information would require a disproportionate effort. In such cases, the data subjects must be informed through publicly published information, or a similar measure must be taken that ensures similarly effective information to the data subjects.

82. If the organization also carries out data processing activities, it shall immediately inform the data controller, for whom it performs the data processing activities, of the data protection incident that occurred at it.

83. If the organization employs a data processor, it must be stipulated in the data processing contract that the data processor is obliged to immediately notify the organization of any data protection incident that has occurred.

XII. Management of customer data

84. The organization carries out its statutory auditor activities based on a written contract pursuant to § 45 of the Civil Code. The legal basis for data management is based on the contract, in relation to the party signing the contract and the personal data relating to it.

85. Personal data that becomes accessible to the organization in the context of the performance of the contract according to the previous point (for example, the contact data included in the contract or personal data that is necessary or deemed necessary to know during the performance of the task in accordance with the legal regulations and professional guidelines and requirements of the auditing activity based on legal obligation { for example, the legal basis for handling member loans is based on the legitimate interest of the organization. In accordance with the provisions of the GDPR, in this case it is necessary to carry out the following interest assessment test:

a) subject of data management
b) establishing the legal basis of the legitimate interest
c) the personal data to be processed
d) purpose of data management
e) designation of the legitimate interest of the organization
f) what rights of the data subjects may be violated
g) consideration of interests
h) what measures and guarantees does the organization apply in order to adequately protect the personal data collected in this way.

86. The interest assessment test(s) carried out regarding the management of the scope of the given personal data are attached to these regulations.

XIII. Employment-related data management

87. The organization shall include the provisions of points 33 and 34 regarding job applications in the "Data Management Information" according to point 36. In the job application it publishes, the organization refers to the "Data Management Information" by indicating the contact information. If the organization did not make the "Data Management Information" available electronically, it includes the relevant provisions in the job application.

88. If the organization wishes to store the documents submitted by the job applicant even after the job application has been filled, the job applicant's consent must be requested. The consent must be voluntary, specific, based on adequate information and clear. For this purpose, the declaration of consent must contain at least the following:

a) the identity and contact details of the representative of the organization;
b) the purpose of the planned processing of personal data [for example, a subsequent request to fill a newly opened position], as well as the legal basis for data processing (consent-based);
c) the duration of storage of personal data;

d) the right of the data subject to request from the organization access to personal data relating to him, their correction, deletion or restriction of processing;

e) the data subject's right to withdraw their consent at any time, which, however, does not affect the legality of the data processing carried out on the basis of the consent prior to the withdrawal;

f) on the right to submit a complaint addressed to the authority.

89. After the evaluation of the application, the data carriers containing the personal data of the unsuccessful applicants must be returned to the applicant within 90 days, upon request, or destroyed in the absence of the applicant's consent to the use of their personal data in further applications. A record of the destruction (deletion) must be taken.

90. The organization manages the employees' data based on the relevant provisions of the Mt. and informs them in the manner specified in the Mt., in compliance with the data management principles contained in the GDPR.

91. The organization provides employees with information about the data processors it uses about their identity and the scope of the data transmitted to them.

92. The following legal bases may typically arise during data processing in the employment relationship:

a) based on a contract [the employment contract]

b) based on legal obligation [e.g. taxation, alimony deduction]

c) based on legitimate interest [for example, data related to workplace inspections].

93. If the organization manages data on the basis of point 92. c), in accordance with the provisions of the GDPR, in this case it is necessary to carry out the following interest assessment test:

i) designation of the legitimate interest of the organization

j) who are the data subjects and what rights are violated

k) consideration of interests

l) what measures and guarantees does the organization apply in order to adequately protect the personal data collected in this way.

94. The interest assessment test(s) carried out regarding the management of the scope of the given personal data must be made available to the employees [for example via an internal network, as an attachment to the employment contract].

XIV. Provisions regarding the use of the data processor

95. If the data management is carried out by someone else on behalf of the organization [for example, payroll, server service, website operation], the organization may only use data processors who provide adequate guarantees that the data management complies with the GDPR requirements and that the rights of the data subjects are protected. and to implement organizational measures.

96. The data processor may not use additional data processors without the organization's prior written authorization or general authorization.

97. The organization and the data processor enter into a contract with regard to the data processing performed by the data processor. This contract defines the subject, duration, nature and

purpose of data management, the type of personal data, the categories of data subjects, as well as the organization's obligations and rights.

98. The contract according to the previous point specifically stipulates that the data processor:

a) personal data is handled solely on the basis of the organization's written instructions,
b) ensures that the persons authorized to handle personal data undertake a confidentiality obligation or are subject to an appropriate confidentiality obligation based on legislation;
c) apply data security measures of at least the level prescribed by the organization;
d) respects the conditions mentioned above regarding the use of the additional data processor;
e) taking into account the nature of the data management, with appropriate technical and organizational measures, it helps the organization to the extent possible to be able to fulfill its obligations with regard to responding to requests related to the exercise of the rights of the data subject;
f) assists the organization in fulfilling its obligations under the data protection incident, taking into account the nature of the data management and the information available to the data processor;
g) agrees to inform the organization immediately in the event of a data protection incident;
h) after the completion of the provision of the data management service, based on the decision of the organization, it deletes or returns all personal data to the organization and deletes existing copies, unless EU or member state law requires the storage of personal data.

99. The data processor and the person with access to personal data may only handle this data in accordance with the organization's instructions.

XIV. Implementing and closing provisions

100. These regulations enter into force on May 25, 2018.

Appendix No. 1

Interest assessment test
– regarding contractual (volunteer, domestic and international program participant) contact data –

Subject of data management: The Tempus Public Foundation, which manages the European Solidarity Corps and the ERASMUS+ European Union programs, during the organization's implementation of the projects managed by it, contacts, contracts, participant reports and the managed data related to the implementation of the project (including preparation, implementation, evaluation and follow-up), the management of certain personal data of persons included in contracts and agreements (hereinafter: contract) (hereinafter: data subjects) for the provision of activities, allowing access for inspection purposes

Legitimate interest legal basis: After examining the provisions of Article 6 of the GDPR, the organization came to the conclusion that the legality of processing the data of the natural persons (data subjects) included in the contract can be based on the legitimate interest of the data controller according to Article 6 (1) f) of the GDPR.

To be treated personal data: The name, telephone number and e-mail address(es) used for communication of the contact person (data subject) according to the contract, as well as a copy of his or her photo identification card. Personal data is made available by the person who signs the contract as a client of the data controller.

Purpose of data management: To maintain contact necessary to fulfill the obligations contained in the contract, to identify the participant's identity and place of residence by country due to the application costs.

Legitimate interest: Facilitation of the organization's effective fulfillment of the terms of the contract, verification of the legality of the use of public funds.

Rights affected, which may be infringed: Right to naming; identification of a natural person based on other data

Consideration of interests: The organization's interest is to carry out its activities as efficiently as possible, to achieve the goal of being able to devote adequate time to the professional fulfillment of its contractual obligations. Administrative tasks and needs related to the fulfillment of the contract (for example, obtaining documents) can be realized and satisfied as efficiently as possible if the organization is in contact with the person responsible for these tasks and competent to perform them. The organization has a relevant and appropriate relationship with the data subject, since the data subject or the organization delegating him has a contractual relationship with the organization.

Guarantees: The organization only processes the data of the data subject in order to fulfill the terms of the contract.
The organization is also bound by the confidentiality provisions contained in the contract.
The organization has a strict internal data management procedure in force, only authorized persons have access to the data; data is not transmitted.

Summary: Based on the above, the organization considers that it can be established that it has a legitimate interest in processing the data of those included in the contract concluded with the participants, that the legitimate interest is not overridden by the rights and freedoms of the individual.

Debrecen, 01 May 2021 Signed by

Andrea Keresztesi, president