Data Processing Notice
on the operation of the internal whistleblowing system

The **Budapest Festival Orchestra Foundation** (registered office: H-1034 Budapest, Selmeci u. 14-16.) ("**BFO**") has appointed **Bozsonyik Law Office** as its whistleblower protection lawyer under a contract to provide whistleblowing services and operate the internal whistleblowing system in accordance with Hungarian Act XXV of 2023 on Complaints, Public Interest Reports and Rules on Whistleblowing ("**Complaints Act**"). Bozsonyik Law Office is an independent controller in relation to whistleblower protection activities ("**Controller**").

The Controller hereby informs the data subjects about the data processing activities related to the above-mentioned activities, in accordance with the provisions of Regulation (EU) No 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 (hereinafter: **GDPR**).

1. Controller:

Name: Bozsonyik Law Office
Represented by: Dr. Hedvig Bozsonyik, Head of Office
Registered office: H-1121 Budapest, Eötvös út 25.
Phone: +36 20 4393264
E-mail: info@bozsonyikpartners.com

2. Purpose and lawful basis of processing, scope of data subjects and the data processed

2.1 Purpose of processing:

Receiving reports made through the internal whistleblowing system, investigating them, maintaining contact with the whistleblower, and remedying or eliminating the conduct that is the subject of the report.

2.2 Lawful basis for processing:

The Controller processes the data relating to the whistleblower on the basis of the whistleblower's consent (Article 6(1)(a) of the GDPR), and other data associated with the report to comply with the legal obligations set out in the Complaints Act, as provided for in Article 6(1)(c) and (f) of the GDPR.

2.3 Scope of data subjects:

- the whistleblower,
- the person or persons whose conduct or omission gave rise to the report,
- the person or persons who may have relevant information about the contents of the report.

2.4 Scope of the data processed:

Pursuant to Section 26(1) of the Complaints Act, within the framework of the whistleblowing system, the fact of the report and the personal data of the data subjects that is essential for investigating the report.

3. Duration of processing

Personal data that is not necessary for conducting the investigation shall be deleted by the Controller without delay.

The Controller shall delete personal data from the investigation documentation immediately upon completion of the investigation, but no later than 30 days thereafter, unless further proceedings are initiated on the basis of the investigation.

If the Controller finds that the whistleblower cannot be identified on the basis of the report and decides not to investigate the report, the Controller shall delete the report and the data contained therein immediately after making the decision not to investigate the report.

If proceedings initiated on the basis of the report establish suspicion of an employment law violation, administrative offense, criminal offense or other violation giving rise to court or other official proceedings, the personal data processed in connection with the investigation shall be processed by the Controller until the final conclusion of the proceedings initiated.

4. Description of technical and organizational measures taken to ensure data storage and data security

The Controller guarantees that its contributors who have access to personal data are subject to confidentiality obligations.

The Controller shall take all reasonable technical precautions to ensure that the stored data are secure and inaccessible to third parties, extending not only to IT security measures but also the physical protection of the premises where the data are stored.

The Controller ensures data security through the following IT security solutions: anti-virus protection, firewall, password protection.

Paper documents are stored in a key-locked location and in lockable fireproof cabinets.

5. Data transfer

The Controller shall send the employer an extract from the report that does not contain any data enabling the identification of the whistleblower, unless the whistleblower has given prior written consent to the transmission of their personal data.

Except in cases of bad faith reporting, the personal data of the whistleblower may only be disclosed to the competent authority conducting proceedings based on the report if that authority is authorized by law to process such data or if the whistleblower has given consent to the transmission of their personal data.

The personal data of the whistleblower shall not be disclosed without their consent.

If it becomes apparent that the whistleblower has provided false information of decisive importance in bad faith and
(a) this gives rise to circumstances indicating that a criminal offense or administrative offense has been committed, their personal data will be transmitted to the authority or person authorized to conduct the proceedings (e.g. investigating authority),
(b) there are reasonable grounds to believe that the whistleblower has caused unlawful damage or other legal harm to another person, their personal data will be transmitted upon request to the authority or person authorized to initiate or conduct the proceedings.

The Controller will not transfer data to third countries or international organizations.

6. Automated decision-making

No automated decision-making takes place during the processing.

7. Rights of data subjects in relation to the processing

In relation to the processing of their personal data, data subjects have the following rights:

(a) **Right of access (Article 15 GDPR)**: the data subject shall have the right to obtain from the Controller information as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the information contained in this Notice.

Upon request, the Controller shall provide the data subject with a copy of the personal data processed. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the Controller shall provide the information in a commonly used electronic form.

Under the Complaints Act, in exercising the right to information and access, the personal data of the whistleblower may not be disclosed to the person requesting the information.

(b) **Right to rectification (Article 16 GDPR)**: the data subject shall have the right to obtain from the Controller without undue delay the rectification of inaccurate personal data concerning him or her; and shall also have the right to have incomplete personal data completed.

(c) **Right to erasure (Article 17 GDPR)**: the data subject shall have the right to obtain from the Controller the erasure of personal data concerning him or her without undue delay and the Controller shall erase personal data without undue delay if (i) the personal data is unlawfully processed by the Controller; (ii) the data subject objects to the processing and there are no overriding legitimate grounds for the processing; (iii) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the Controller is subject; (iv) the personal data are no longer necessary in relation to the purposes for which they were collected by the Controller.

The above provisions of this paragraph (c) shall not apply to the extent that processing is necessary (i) for compliance with a legal obligation which requires processing of personal data

by Union or Member State law to which the Controller is subject, or (ii) for the establishment, exercise or defense of legal claims.

(d) **Right to restriction of processing (Article 18 GDPR)**: the data subject shall have the right to obtain from the Controller restriction of processing where for example (i) 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; (ii) the Controller no longer needs 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; (iii) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead; or (iv) the data subject has objected to processing pending the verification whether the legitimate grounds of the Controller override those of the data subject.

(e) **Right to object** (Article 21 GDPR): the data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of his or her personal data necessary for the performance of a task carried out by the Controller or by a third party on the basis of the legitimate interests of the Controller or a third party. In this case, the Controller shall no longer process the personal data unless the Controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defense of legal claims.

(f) **Right to information regarding the above-mentioned rights (Article 12 GDPR)**: within one month of receipt of the data subject's request under paragraphs (a) to (e) above, the Controller shall inform the data subject of the circumstances of the processing. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The Controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay.

The information shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, taking into account the administrative costs of providing the information or communication or taking the action requested, the Controller may either (i) charge a reasonable fee; or (ii) refuse to act on the request.

(g) **Right to lodge a complaint (Article 77 GDPR)**: the data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement, if the data subject considers that the processing of personal data relating to him or her infringes the law on data processing. Complaints may be lodged with the National Authority for Data Protection and Freedom of Information (address: H-1055 Budapest, Falk Miksa u. 9-11.; phone: +36 1 391 1400; fax: +36 1 391 1410; mailing address: H-1363 Budapest, Pf.: 9.; www.naih.hu; email: ugyfelszolgalat@naih.hu).

(h) **Right to judicial remedy (Article 79 GDPR)**: the data subject shall have the right to seek judicial remedy where he or she considers that his or her rights have been infringed as a result of the processing of his or her personal data in non-compliance with the law. Proceedings against a controller shall be brought before the courts of the Member State where the controller

has an establishment, but such proceedings may also be brought before the courts of the Member State where the data subject has his or her habitual residence.

Terms:

This Notice uses the terms defined in the GDPR and the Complaints Act.

"Personal data" means 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;

"Processing" means 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, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

"Controller" means the 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;

"Processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

"Whistleblower" means the person who makes the report.

"Employer" means the person who employs a natural person under an employment relationship.

Budapest, 1 June 2025