

General Director's Instruction No. 10/2022
on the issuance of the Data Protection Policy

Pursuant to my internal regulatory power as defined in Sec. 32. of the Organizational and Operational Rules (hereinafter: **OOR**) of the Hungarian State Opera (hereinafter: **OPERA**), I hereby order the following employer's measures:

1. By issuing this instruction, I enact the "**Data Protection Policy (V2)**" regulation, as annexed to this instruction.
2. This instruction will be announced in the form of a circular email, and published in the IT system of the OPERA.
3. This instruction will **enter into force on 20 June 2022**, and the following regulation shall be repealed:
 - a) Internal Privacy Policy (V1) regulation published with General Director's Instruction No. 14/2018,
 - b) DigiWTime Privacy Policy (V1) regulation published with General Director's Instruction No. 3/2018,
 - c) Andoc Privacy Policy (V1) regulation published with General Director's Instruction No 2/2018.

Budapest, "according to time stamp"

Hungarian State Opera
ÓKOVÁCS Szilveszter
Director General

Dr. FŐZŐ Virág
Deputy Director General

Table of contents

GENERAL PROVISIONS	3
1. The purpose of this Policy	3
2. Applicable legislation.....	3
3. Definitions	3
4. General principles relating to processing of personal data	4
DETAILED PROVISIONS	5
5. Data Protection.....	5
6. Provisions for the Data Protection Officer	5
7. Disclosure of personal data, data transfer.....	6
8. Procedures applicable in cases of data breach.....	7
9. Procedures applicable to the exercise of data subject rights	7
FINAL PROVISIONS	8
10. Revision	8
11. Review process	8

Data Protection Policy

Version No.: V2

GENERAL PROVISIONS

1. The purpose of this Policy

- 1.1. The purpose of this Policy is to establish the key regulations of data processing done within the OPERA, and to record the appropriate procedures in order to comply with current privacy laws.

2. Applicable legislation

- 2.1. The present policy shall be interpreted in accordance with the following legislation:
- a) Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter referred to as **GDPR**),
 - b) Act CXII of 2011 on informational self-determination and freedom of information (hereinafter referred to as **Infotv.**),
 - c) Act I of 2012 on the Labour Code (hereinafter referred to as **Mt.**).

3. Definitions

- 3.1. For the purposes of the present Policy:¹
- a) **personal data:** *any information relating to an identified or identifiable natural person; 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) **data processing:** *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) **data controller:** 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,
 - d) **data processor:** a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller
 - e) **data transfer:** the sending of personal data to a third party, sharing the data with them or making the data accessible by them,

¹ In accordance with article 4 of the GDPR.

- f) **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,
- g) **data subject:** an identified or identifiable natural person to whom the personal data relates,
- h) **supervisory authority:** National Authority For Data Protection And Freedom Of Information,
- i) **third party:** a natural or legal person, public authority, agency or body other than the data subject, the OPERA, processor and persons who, under the direct authority of the OPERA, are authorised to process personal data.

4. General principles relating to processing of personal data

- 4.1. During the processing of personal data, the following principles shall be considered especially.
 - a) **Lawfulness, fairness and transparency:** personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.
 - b) **Purpose limitation:** personal data shall be collected for specified, explicit and legitimate purposes only.
 - c) **Data minimisation:** personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
 - d) **Storage limitation:** personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods only in cases provided for by law.
 - e) **Integrity and confidentiality:** personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- 4.2. In line with the applicable legislation, the OPERA is responsible for complying with the principles, and according to the principle of **accountability**, it must be able to verify this compliance, therefore every employee involved in data processing must comply with the provisions of the present policy.
- 4.3. According to the principle of transparency, the OPERA informs its employees in a separate document comprehensively and in detail about the processing of their personal data relevant to their employment, and provides information to the data subjects as necessary on a case-by-case basis for other instances of data processing.
- 4.4. The employee processing the data shall only process personal data following the OPERA's instruction, complying with the provisions of internal regulatory devices (Bylaws, written instructions, policies), job descriptions or written procedures, except in cases when they are obliged by law to do otherwise.
- 4.5. It is forbidden to process data without complying with the provisions of the present policy and the GDPR warranties, it is in particular forbidden to create separate data bases, data sheets containing personal data in any form, even if it would serve the interests of the OPERA. Such data bases, data sheets must be deleted.
- 4.6. In case of the processing of third parties' personal data (e.g. in connection with events, prize games), the data protection officer must be consulted before the data processing starts.

DETAILED PROVISIONS

5. Data Protection

- 5.1. The OPERA ensures the physical, logical and administrative protection of the controlled personal data according to the **principle of integrity and confidentiality**.
- 5.2. In order to ensure **physical protection**, the OPERA
- a) issues a policy describing the procedures of access control and key management;
 - b) in justified cases ensures manned guarding,
 - c) in the absence of or in addition to that, it ensures the operation of the electronic surveillance system (camera system) and access control system,
 - d) provides and enforces appropriate fire safety regulations,
 - e) stores the documents containing personal data in offices that can be locked.
- 5.3. In order to ensure **logical protection**,
- a) the OPERA creates an IT security policy, in which it lays down the rules of access management and protection, and defines the rules of archiving, saving, virus protection, e-mail security, software usage, remote access control, mobile IT activities, the use of mobile devices and the handling of printers,
 - b) the IT Department ensures the creation of back-up copies and the virus protection of data carriers containing personal data, and protects it from unauthorised access through appropriate authentication processes,
 - c) the IT Department takes appropriate measures to ensure that the principles of data protection and data security are properly complied with even in the case of remote work, in particular regarding the minimisation of the risk of unauthorised access.
- 5.4. In order to ensure **administrative protection**,
- a) the OPERA provides that the personal data controlled by it shall only be accessed by employees working in specific roles, within the scope of their functions recorded in their job description, and with appropriate reason and legal basis,
 - b) the OPERA provides that personal data shall only be collected in compliance with the principle of purpose limitation,
 - c) for roles involving the regular processing of personal data, internal trainings are organised regularly or in justified cases by the human resources specialist responsible for training and development in cooperation with the data protection officer.
- 5.5. The person authorised to act in the capacity of employer may access data relevant to the employment relationship stored on an IT device used to carry out their work.² The present paragraph also applies to cases when the parties agree that the employees use their own IT devices in order to carry out their work.

6. Provisions for the Data Protection Officer

- 6.1. The General Director of the OPERA designates a Data Protection Officer through a specific measure.

² Paragraphs §11/A.(3), (5) of Mt

- 6.2. Regarding the position of the Data Protection Officer, the OPERA properly complies with the provisions of Chapter 4 of the GDPR, in particular the following provisions.
- 6.3. The OPERA shall publish the name and contact details of the Data Protection Officer through the Data Protection Officer, and communicate them to the supervisory authority.
- 6.4. The OPERA ensures that the Data Protection Officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data. To this end, every employee is obliged to cooperate with the Data Protection Officer.
- 6.5. The Data Protection Officer may fulfil other tasks and duties as the employee of the OPERA. The OPERA shall ensure that any such tasks and duties do not result in a conflict of interests.
- 6.6. The OPERA provides a separate email account (dpo@opera.hu) for the Data Protection Officer to carry out their tasks and duties.
- 6.7. The OPERA shall support the Data Protection Officer in performing the tasks referred to in the present section by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain their expert knowledge.
- 6.8. The Data Protection Officer performs the tasks referred to in Article 39 of the GDPR, in particular the following:
 - a) inform and advise (including the preparation of privacy policies) the management and the employees of the Opera who carry out processing of their obligations pursuant to the applicable data protection provisions;
 - b) monitor compliance with applicable laws and the present Policy, the awareness-raising and training of staff involved in processing operations, and the related audits;
 - c) cooperate with the supervisory authority.
- 6.9. According to the principle of accountability, the Data Protection Officer shall
 - a) keep record of the privacy policies issued with the help of the filing and contract management systems,
 - b) keep record of data transfers,
 - c) keep record of data breaches,
 - d) and keep record of the exercise of data subject rights.
- 6.10. The OPERA informs its employees in a separate document about personal data processing that involves them.
- 6.11. The Data Protection Officer shall cooperate with an employee authorised to edit the www.opera.hu website to ensure that privacy policies applicable to third parties are accessible through the website.

7. Disclosure of personal data, data transfer

- 7.1. In case a request is made by a person outside of the OPERA's organisation (hereinafter referred to as third party) involving the disclosure, transfer of personal data, the addressee of the request judges the admissibility of the transfer considering the principles defined in the present Policy, and consults the Data Protection Officer if necessary. Data subjects shall be informed about the transfer of their data.
- 7.2. When necessary, the Data Protection Officer gives advice about the acceptability of the data transfer and informs the data subjects about it.
- 7.3. In case of data transfers involving a larger amount of personal data or their transfer to third countries or international organisations, the prior opinion of the Data Protection Officer shall be sought.

- 7.4. The data subject shall be informed about data transfers required by the tax authority or other authorities in a recallable written format, unless the informing of the data subject is likely to prevent or seriously hinder the achievement of the purposes of the procedures carried out by the authority.³ The decision relevant to that has to be noted at the time of the reply sent to the authority.
- 7.5. Points 7.1-7.4. do not need to be applied in cases when the transfer of personal data is done by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.⁴

8. Procedures applicable in cases of data breach

- 8.1. A person becoming aware of a data breach is obliged to notify the Data Protection Officer **without undue delay, not later than the following working day** in person, or via telephone by calling +36 1 814 7444, or by sending an email to dpo@opera.hu. Where the notification is not made within the time limit defined above, it shall be accompanied by reasons for the delay.
- 8.2. If someone is unable to judge whether a certain event or issue qualifies as data breach or not, they are obliged to report the event or issue considered problematic by them to the Data Protection Officer in the same way as described above.
- 8.3. If the Data Protection Officer finds that the given event qualifies as a data breach, they inform the following persons about the reported issue **without undue delay**:
- the Director General (through the Deputy Director General)
 - the Head of Legal and Human Resources Department,
 - the Senior Legal Advisor,
 - the Head of the IT Department,
 - and the head of the organisational unit involved in the data breach.
- 8.4. The Data Protection Officer and the notified persons (hereinafter collectively referred to as the **data protection crisis team**) led by the Data Protection Officer—following the procedures provided by the GDPR—categorise the breach as a first step, i.e. determine its impact on the rights and freedom of the natural persons involved (*1. high risk, 2. risk, 3. no risk*).
- 8.5. After that, the Data Protection Officer shall **report the breach not later than 72 hours after having become aware of it** via the platform provided by the supervisory authority. Where the notification is not made within the time limit defined above, it shall be accompanied by reasons for the delay.
- 8.6. When the personal data breach is likely to result in a **high risk** to the rights and freedoms of natural persons—as determined by the data protection crisis team—the Data Protection Officer shall notify the data subject too in the name of the Director General of the OPERA without undue delay, unless they have implemented appropriate technical and organisational protection measures to the personal data affected by the personal data breach, or unless they have taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise.

9. Procedures applicable to the exercise of data subject rights

³ Article 15(5)(b) of the GDPR

⁴ Article 2(2)(d) of the GDPR

- 9.1. It shall be considered the exercise of data subject rights if relevant to any data processing performed by the OPERA a request is made by the data subject involving the data subject rights recorded in Articles 12–23 of the GDPR.⁵
- 9.2. The addressee of the request for exercising data subject rights shall notify the Data Protection Officer without undue delay, no later than the following working day via telephone by calling +36 1 814 7444, or by sending an email to dpo@opera.hu.
- 9.3. In case the Data Protection Officer finds the given request justified, they carry out the requested measure together with the addressee of the request without undue delay, no later than the time limit set by the Privacy Policy.

FINAL PROVISIONS

10. Revision

- 10.1. Following the date of its entry into force, the present Policy shall be revised every year by January 31st, or in case the circumstances or the legal framework are significantly changed.

11. Review process

- 11.1. The present Policy has been reviewed in full compliance with the “Policy on the rules of forming and updating internal policies” issued via Director General No. 5/2017, and thereafter being submitted for approval, and approved.

⁵ Typically the request of some measure, in particular: requesting information, requesting access to their own personal data, requesting rectification, erasure, or restriction of processing, making an objection etc. (hereinafter referred to as **the exercise of data subject rights**).