MAGYAR ÁLLAMI OPERAHÁZ
HUNGARIAN STATE OPERA

PRIVACY POLICY
~ concerning the personal data processed in the course of operating the electronic surveillance system at the *Rehearsal Studio*~

Data Controller:	**The Hungarian State Opera**
Registered and mailing address:	1061 Budapest, Andrássy út 22.
Place of processing:	1066 Budapest, Jókai utca 4. **(Rehearsal Studio)**
Website:	www.opera.hu
Data protection officer contact information:	dpo@opera.hu 06 1 814 7444
Those of the data controller's employees can access the personal data processed in the course of operating the electronic surveillance system for whom such access is essential for the performance of their tasks. These persons include the data controller's General Director and Deputy General Director, the employees of the Legal Department, the employees of the Facility Management Department, the employees of the IT Department, and the Safety Technology Coordinator.	
The purpose of data processing:	**to provide property protection and to prevent and detect unlawful actions.**
The source of personal data:	the data subject.
Retention period – electronic surveillance system:	camera recordings are retained for 7 days from the time of their recording, after which time they are automatically deleted;
The 7-day retention period for recorded videos is the same as the length of uninterrupted video that the system can store continuously. *The retention period also protects the rights of data subjects, as data subjects also have 7 days to request the restriction (blocking), retention and release of their personal data.* *The controller considers that a retention period of 7 days is sufficient, necessary and proportionate, is in line with the objectives of the electronic monitoring system and serves the legitimate interests of both the controller and the data subjects, as well as the authorities and courts involved in any enforcement proceedings.*	
Data processor:	**T.O.M. Controll 2001 Vagyonvédelmi és Szolgáltató Zártkörűen Működő Részvénytársaság**
Registered address:	1038 Budapest, Ráby Mátyás u. 26.
Company registration number:	01-10-046929
Tax number:	14883664-2-41

Contact information:	info@tomcontroll.hu
The data controller selected the company that deals with property protection by way of a public procurement procedure conducted in line with the rules of Act CXLIII of 2015 on Public Procurement (hereinafter: Public Procurement Act); the company provides property protection, reception, cash security, cash transport, and patrol services at the Hungarian State Opera's venues and sites, in the course of which it processes the personal data of data subjects as the data processor.	
Rights of data subjects:	right of access, right to rectification, right to erasure, right to restriction of processing, right to object, Right to an effective judicial remedy against the employer or data processor:

Right of access

The data subject has the right to obtain from the data controller confirmation as to whether or not personal data concerning it are being processed. If such processing takes place, the data subject is entitled to receive access to the personal data and the following information:

- *the purposes of the processing;*
- *the categories of personal data concerned;*
- *the recipients or categories of recipient to whom the personal data have been or will be disclosed by the data controller, in particular recipients in third countries or international organisations;*
- *where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;*
- *the existence of the right to request from the data controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;*
- *the right to lodge a complaint with a supervisory authority; and*
- *where the personal data are not collected from the data subject, any available information as to their source; h) the existence of automated decision-making (Article 22 (1) and (4) of the GDPR), including profiling, and, at least in these cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.*

The data processor shall make a copy of the personal data subject to processing available to the data subject. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

Right to rectification

The data subject shall have the right to obtain from the data controller without undue delay the rectification of inaccurate personal data concerning him or her. The data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

Right to erasure ('right to be forgotten')

The data subject has the right to obtain from the data controller the erasure of personal data concerning it and the data controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

- *the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed by the data controller;*
- *the data subject objects to the processing and there are no overriding legitimate grounds for the processing;*
- *the personal data were processed unlawfully;*
- *the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the data controller is subject;*

Where the data controller has made the personal data public and is obliged pursuant to the above to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such data controllers of, or copy or replication of, those personal data.

The above provisions shall not apply if data processing is necessary, among others:

- *for exercising the right of freedom of expression and information;*
- *for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject;*
- *for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or*
- *for the establishment, exercise or defence of legal claims.*

Right to restriction of processing

The data subject shall have the right to obtain from the data controller restriction of processing where one of the following applies:

- *the accuracy of the personal data is contested by the data subject, for a period enabling the data controller to verify the accuracy of the personal data;*
- *the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;*
- *the data 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 defence of legal claims;*
- *the data subject has objected to processing pending the verification whether the legitimate grounds of the data controller override those of the data subject.*

Where processing has been restricted as set out above, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

A data subject who has obtained restriction of processing shall be informed by the data controller before the restriction of processing is lifted.

Notification obligation regarding rectification or erasure of personal data or restriction of processing

The data controller shall communicate any rectification or erasure of personal data or restriction of processing to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.

Right to object
The data subject has the right to object, on grounds relating to its particular situation, at any time to processing of personal data concerning it based on a legitimate interest. In this case, the data controller shall no longer process the personal data unless it demonstrates compelling legitimate grounds for the processing which override the data subject's interests, rights, and freedoms or for the establishment, exercise or defence of legal claims. *Where personal data are processed for scientific or historical research purposes or statistical purposes, the data subject, on grounds relating to its particular situation, shall have the right to object to processing of personal data concerning it, unless the processing is necessary for the performance of a task carried out for reasons of public interest.*
Submitting a complaint to the supervisory authority
The data subject is entitled to submit a complaint at the supervisory authority if it feels that the processing of the data pertaining to the data subject is in violation of the provisions of the GDPR. *The competent supervisory authority in Hungary:* ***Nemzeti Adatvédelmi és Információszabadság Hatóság [Hungarian National Authority for Data Protection and Freedom of Information]*** *Website: http://naih.hu/* *Address: 1125 Budapest, Szilágyi Erzsébet fasor 22/c;* *Postal address: 1530 Budapest, Pf.: 5.;* *Phone: +36-1-391- 1400;* *Fax: +36-1-391-1410;* *Email: ugyfelszolgalat@naih.hu*
Right to an effective judicial remedy against a supervisory authority
The data subject shall have the right to effective judicial remedy against a legally binding decision of a supervisory authority concerning it. *The data subject shall have the right to effective judicial remedy where the competent supervisory authority does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint lodged.* *Proceedings against a supervisory authority shall be brought before the competent court of the Member State where the supervisory authority is established.*
Right to an effective judicial remedy against the employer or data processor:
Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority, the data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under the GDPR have been infringed as a result of the processing of his or her personal data in non-compliance with the GDPR. *Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence. In Hungary, such cases fall under the jurisdiction of tribunals. The action shall be heard by the competent tribunal. If so requested by the data subject, the action may be brought before the tribunal in whose jurisdiction the data subject's home address or temporary residence is located. Information on the jurisdiction of the court and contact information of the court is available on the following website: www.birosag.hu.*

The following may be incurred in connection with the rights and right to remedy of data	The right to rectification is primarily due the data subjects in connection with the time of recording

subjects, stemming from the features of the electronic surveillance system:	(in light of the fact that the content of the recordings can obviously not be rectified). The data subject's right to access, thus including the right to receive copies, may be exercised only in a manner that does not adversely affect the rights and freedoms of others. The length of the period affected by the copy is restricted to the reasonable duration of the time, duration, action, or event that affects the data subject. As part of the right to access, the data subject may, in addition to requesting a copy, request information pertaining to the exact times between which he or she is visible on the recordings, what actions were recorded, and whether any action takes/took place involving or affecting the data subject after he or she is no longer visible on the recording. The data subject may request to inspect the recordings that involve him or her. The data controller complies with the right of inspection at the address specified in this policy, at a time agreed on beforehand. In a specific case, the data controller shall specify the exact room depending on free capacities, at a reasonable time prior to inspection.
Data security:	
Data security measures:	
The data controller's collaborators and employees participating in data processing are entitled to learn of the personal data to the degree specified beforehand, with the specification of permission levels, subject to undertaking an obligation of confidentiality. *Personal data are protected by suitable technical, logical, and administrative measures, we ensure that the data are secure and available, and we protect those from unauthorised access, alteration, damage, and disclosure, as well as all other forms of unauthorised use.* *Organisational measures are used to examine the possibilities of physical access to buildings, our employees are continuously trained, and hard copy documents are kept locked away with suitable protection. Technical measures include the use of encryption, password protection, and anti-virus software. The company does everything it can to make the processes as secure as possible; strict regulations are observed as regards the data received by the Company in the interest of maintaining the security of data and preventing illegal access.*	
Data security in the IT infrastructure:	
The company has detailed internal regulations in place that extend to all details relevant from the aspect of data security and that include data security as well as information security provisions. *Personal data are stored on servers located at own sites. Strict security measures are put in place to ensure that unauthorised persons cannot physically access the system.* *Data storage media are kept in locked, climate-controlled rooms.* *No backup is made of the data recorded by the electronic surveillance system.* *Access to the servers is possible only through the internal IT network, after identification with a user name and password. The IT systems are tested from time to time, recurrently, and regularly to ensure and maintain data and IT security.*	

The use of network resources by users is regulated, restricted, and requires identification. *The office workstations can only be used in possession of the correct user name and password. Foreign data media can only be used following an automatic scan for viruses and other malware.* *We continuously ensure the protection of the data controller's systems and components against malicious software.* *Security functions are given priority and handled separately during the planning, development, testing, and operation of programs, applications, and tools.* *The passkeys (e.g. password) for accessing the information system are stored in the system with restricted access requiring the user to log in; data affecting the safety of the system (e.g. passwords, entitlements, logs) are ensured protection when allocating access rights.*
Physical data security:
In the interest of the physical security of data, we ensure that doors and windows lock properly and offer adequate protection, with strict visiting and entry protocols in place for visitors. An alarm system is used to guarantee property protection. The site is guarded around the clock. *Hard copy documents that contain personal data are kept in a locked cabinet that guarantees property protection; only a specified sphere of individuals have access with the suitable management of privileges.* *The rooms for housing data storage media have been developed in a manner that guarantees sufficient security against unauthorised access, access by force, fire, and natural disasters. Data media used for transferring, saving, and archiving data are stored only in locked locations that offer suitable protection.*
Procedure put in place for data breaches:
In line with the provisions of relevant legislation, data breaches are reported to the supervisory authority within 72 hours of learning thereof, and records are kept of data breaches. Data subjects are also informed in the cases specified by law.

If the sphere of managed data or any other circumstance related to data management changes or is amended, the data controller shall amend this Privacy Policy and publish it in the customary manner.

This Privacy Policy is available both on the data controller's internal IT network and on its website.

Budapest, [as per the timestamp]

The Hungarian State Opera

Annexes:

1. Annex: Locations of cameras
2. Annex: The angle of views of cameras
3. Annex: Balance of interests
4. Annex: Data protection impact assessment
5. Annex: Data breach records - sample
6. Annex: Records of inspections of electronic surveillance data - sample

1.

SZÍNPAD
83,00 m²

14,70

2.

1.sor
2.
3.
4.
5.
6.
7.
8.
9.
10.
11.

V. fokt.

Közlekedő

Szálloda gazd. bejárat

Kuka tároló

Új szálloda

bejárat

Gazd. bejárat légtere

Iroda

női WC

női WC

előtér

ffi. WC

ffi. WC

előtér

öltöző

közl.

közlekedő

Szolgalmi út

Vészkijárat

Porta

lift

Előtér

Raktár

Iroda

Iroda

Iroda

Iroda

Telefon központ

Tároló

Lépcső

Jókai utcai bejárat

lép

bejára

2020. XI. 18. LÁO

3.
4.
8.
9.
10.
5.
6.
7.
SZÍNHÁZTEREM
326,00 m²
14
31,10
5,07
ELŐCSARNOK
125,00 m²
13
12,50
Előtér
4,00 m²
2,51
12
2,72
ffi WC
6,00 m²
1,25
0,87
Előtér
3,00 m²
női
WC
11
7,60 m²
1,07
0,82
Feljárati lépcső
mellékl.
6,88 m²
1,24
10
raktár
2,25 m²
9
Büfé
17,10 m²
8
3,39
4,29
12,50
raktár
1,30 m²
7
1,58
1,22
2,90
raktár
6,00 m²
6
2,76
előtér
1,20 m²
1,65
1,19
90
5
4,00
5,57
0,55
0,78
lift
4,00
15,90
DÓZSA TEREM
185,20 m²
15
lépcsőház
bejárat
Háztelugyelő
Főlépcső
11,65
2
Előtér
40,70 m²
3
Ruhatár
37,00 m²
7,60
Szélfogó
1,85
Öltöző
13,70 m²
4
4,99
4,22
1
Bejárat 8,4 m²
Zuhanyzó
7,00 m²
4
2,80
Főkapcsoló
lókai utcai bejárat
2020. XI. 18. Lüo

Annex 2 - Rehearsal Studio - camera locations

Serial	Type	Resolution	View	Area observed
1.	IP turret camera (ICR, DWDR, 3d DNR,	4 MP	100°	stage
2.	IP turret camera (ICR, DWDR, 3d DNR,	4 MP	100°	instrument warehouse
3.	IP turret camera (ICR, DWDR, 3d DNR,	4 MP	100°	theatre room
4.	IP turret camera (ICR, DWDR, 3d DNR,	4 MP	100°	stairs
5.	IP turret camera (ICR, DWDR, 3d DNR,	4 MP	100°	lobby
6.	IP turret camera (ICR, DWDR, 3d DNR,	4 MP	100°	entrance
7.	IP turret camera (ICR, DWDR, 3d DNR,	4 MP	100°	Dózsa Room
8.	IP turret camera (ICR, DWDR, 3d DNR,	4 MP	100°	theatre room
9.	IP turret camera (ICR, DWDR, 3d DNR,	4 MP	100°	hall
10.	IP turret camera (ICR, DWDR, 3d DNR,	4 MP	100°	lobby

Annex 3

BALANCE OF INTERESTS
pertaining to the electronic surveillance system installed at the rehearsal studio in Jókai utca

Data subjects and the sphere of persons involved in data processing:

As regards the operation of the electronic surveillance system, all natural persons who enter and stay in the Rehearsal Studio, also including the employees of the Hungarian State Operas and the artists employed by it in the form of agency contracts, qualify as involved in data processing.

The sphere of processed personal data: the video recordings recorded by the electronic surveillance system, the data subject's conduct on the recordings, and the conclusions that can be drawn from those (e.g. the perpetration of a crime);

Purpose and duration of data processing:

The data controller processes the personal data for the purposes of property protection and in the interest of preventing and detecting possible unlawful actions.

The data controller retains the recordings for 7 days from the time of recording, after which they are automatically deleted. When determining the retention period, the data controller took the following into consideration:

- the retention time has to be sufficient for the data controller to learn of any damages or losses suffered by the property in the observed area;
- the data controller has to learn of any violations;
- in case of a violation, it must be possible to launch the necessary court or official proceedings, to use the recordings in the proceedings as evidence, and for the recordings to be suitable for effectively supporting the official or enforcement procedure
- the system is capable of retaining 7 days of continuous recordings.

Why is data processing in the interest of data subjects?

Respect of the data subject's personality rights, thus especially his/her right to his/her image, which the data controller took into consideration to the greatest possible extent when designing the electronic surveillance system, prior to its installation. The data controller complies with the provisions of the information and recommendations provided by the Hungarian National Authority for Data Protection and Freedom of Information (NAIH), i.e. it has not installed any cameras in any rooms where surveillance may violate human dignity, thus especially in dressing rooms, showers, toilets, medical rooms, and waiting rooms. Moreover, it does not use an electronic surveillance system in any rooms that has been designated for employees to use during breaks.

What is the data controller's legitimate interest in connection with processing?

Protection of the state-owned high-value assets listed herein: the furniture, instruments, sheet music, documents, and other unnamed valuable equipment kept in the observed area;

protection of intellectual property;

In connection with the above, recording any crimes, infringements, damages, and the related violations, supporting the related enforcement of rights, clarifying the question of liability, and assisting data subjects.

Why does the data controller's legitimate interest proportionality restrict the rights and freedoms of data subject?

- the recordings do not serve, even indirectly, to check or stimulate the working schedules of employees or the intensity or quality of their work;
- the surveillance system is used only on the data controller's private property, and it is not used to make any recordings of public areas;

- the data controller's control activity and the equipment and methods used do not violate human dignity, thus especially the surveillance system is not used in any locations where they may violate human dignity (e.g. bathrooms, break rooms, massage rooms, etc.);
- the surveillance system is used only in the field of vision/area specified in the annex to the Privacy Policy attached to this data processing activity description, where and to the extent its use is essential in the interest of the realisation of the above data processing goals;
- only the persons specified in the Privacy Policy are entitled to access the recordings;
- all persons who operate and who have access to the electronic surveillance system have participated in training that extends to the requirements of data protection and data security;
- the data controller uses the data security measures specified in the Privacy Policy to protect the personality rights of data subjects, and informs data subjects of the technical measures used with the use of the Privacy Policy;
- the data controller may use any recordings containing proof of violations for the purposes of investigating such violation or for any court or other official procedures in relation thereto if the violation cannot be proven with any other means that affect personal data to a lesser degree (e.g. written document, testimony of witnesses), if its use is essential to enforce the data controller's claim or for successful defence in legal proceedings, and in this respect the data controller's legitimate interests are given priority over the legitimate interests of the data subject;
- The recordings that provide proof of a crime, infringement, or damages may only be used if absolutely necessary for the enforcement of the legitimate interests of the data controller or a third party and if the legitimate interests of the data controller or third party supersede those of the data subject, or if the data controller is obligated by law to use the recording;
- the data controller shall document in writing all inspections of the recording and any issuance of the recording to third parties.

Is the use of the electronic surveillance system absolutely necessary, or are other solutions available that enable the realisation of the planned goal without the processing of personal data or that require the processing of less personal data?

It is primarily the artists employed by the Hungarian State Opera who conduct activities (rehearsals) in the property located at Jókai utca 4. (Ferencsik Room), and this is where the Orchestra Director's and the Orchestra Secretariat Offices and a home stage (Dózsa Stage) are located. An instrument storeroom can be accessed by way of the rehearsal studio, which is used to access valuable handmade instruments. The property also includes additional valuable equipment and devices necessary for day-to-day operations. The round-the-clock guarding of the area (which would otherwise be an alternative method of property protection and that would not result in video recordings and thus the processing of personal data) cannot be feasibly guaranteed. However, economic operation is a condition in light of the fact that the property's asset manager uses state funds.

Due to the fact that property protection targets and the recording of any possible crimes, infringements, damages, and the related violations receive priority for the purposes of the subsequent enforcement of rights, assisting data subjects, and clarifying liability, which priority cannot be guaranteed with the use of any other available technical solutions, the use of the electronic surveillance system is necessary and cannot be avoided.

What guarantees does the data controller use to ensure that the privacy rights of data subjects are affected by camera-based surveillance to the necessary extent only?

- the system does not make it possible to make high-resolution close up shots, and is not suitable for zooming;
- after careful consideration, the data controller has decided to retain the recordings for 7 days, after which the system settings guarantee that they are automatically deleted;
- the quality of the recordings made with the use of the electronic surveillance system is average;

- no cameras have been installed in the rooms used by employees for resting or eating, or in bathrooms and massage rooms;
- the data controller does not use any face recognition technologies when using the surveillance system;
- the data controller does not connect the electronic surveillance system with any other automated security systems;
- the data controller has placed signs at all entrances to the property calling attention to the fact that video surveillance is under way.

Annex 4:

DATA PROTECTION IMPACT ASSESSMENT

pertaining to the electronic surveillance system installed at the rehearsal studio in Jókai utca

Data Controller:

THE HUNGARIAN STATE OPERA

Registered address:	**1061 Budapest, Andrássy út 22.**
Website:	**www.opera.hu**
Registry ID:	**309435**
Tax number:	**15309439-2-42**
Email address:	**dpo@opera.hu**
Represented by:	**Szilveszter Ókovács, General Director**

Data processor:

T.O.M. Controll 2001 Vagyonvédelmi és Szolgáltató Zártkörűen Működő Részvénytársaság

(access to the personal data recorded by the electronic surveillance system)

Registered address:	**1038 Budapest, Ráby Mátyás u. 26.**
Company registration number:	**01-10-046929**
Tax number:	**14883664-2-41**
Email address:	**info@tomcontroll.hu**
Represented by:	**Krisztina Kozák, CEO**

Data and information pertaining to planned data processing:

The purpose of data processing: property protection, prevention and detection of unlawful actions

Data processing actions: monitoring and recording entry to the Rehearsal Studio, staying within the site, and movements within the area

Data processing method: data processing is automatic

The sphere of personal data involved in data processing:

images of the people who enter and stay in the Rehearsal Studio, including the data controller's employees

Justification of necessity and proportionality:

The data controller is a body that performs public functions and managed funds of the Hungarian State. The public task it performs is a performing art, which entails the use and storage by artists in the Rehearsal Studio of valuable handmade instruments and other, also valuable instruments and sheet music that are owned by the Hungarian State and are entrusted to the asset management of the data controller. The property also includes offices containing documents, office furniture, and IT equipment. Due to the size and layout of the area in question, the property protection of the valuable equipment cannot be ensured in any other manner: its protection by live guards only would result in a disproportionately high cost.

The term of storing personal data 7 days

Tools used for data processing:

IT network, server for recording, client computers

Applicable standard and code of conduct:

none

Traceability of data processing:

Can access to personal data be restricted	**yes**	no
Can access to personal data be logged	yes	**no**
Can changes to personal data be logged	yes	**no**
Are the stored data protected against unauthorised access	**yes**	no
Are the stored data protected against destruction and loss	**yes**	no

Measures in support of the rights of data subjects:

Is information provided on data processing?	**yes**	no
Is the right of access ensured?	**yes**	no
Are the rights to rectification and to erasure ensured?	**yes**	no
Is the right to object and the restriction of processing ensured?	**yes**	no
Are data forwarded domestically?	yes	**no**
Are data forwarded internationally?	yes	**no**

Checking the existing impact assessment:

Is an impact assessment available for this data processing?	yes	**no**
Is an impact assessment available for similar actions?	yes	**no**
If yes, can it be used?	yes	no

Justification:

Classification of data processing according to risk category:

Is the methodological or detailed evaluation of the personal attributes of employees processed on the basis of automated methods, thus also including profiling?

yes **no**

Are any special personal data categories subjected to processing?

- race or ethnic origin
- political opinion
- religious or philosophical beliefs
- trade union membership
- genetic or biometric data

- health data
- sexual behaviour or sexual orientation

yes **no**

Are public areas extensively monitored with the use of methodical methods? yes **no**

Are employees subjected to evaluation, scoring, profiling, or forecasting?

yes **no**

Are any automated decision-making processes in place that result in legal or similar effects: data processing aimed at producing legal effects concerning the natural person or similarly significantly affect the natural person?

yes **no**

Is there methodological surveillance: data processing or collection for the surveillance, tracking, or checking of data subjects, or the methodological observation of public areas?

yes **no**

Is data processing on a large scale

- as regards the specific number of data subjects or proportionate to the population
- the amount or the types of data processed
- the term of permanent nature of data processing
- The geographical extent of the processing activity

yes no

Are data sets mapped or combined with each other? yes **no**

Are the data of subordinates and supervisors processed? **yes** no

Are new technologies used or are organisational methods used or applied in innovative ways? If yes, please elaborate. yes **no**

Does data processing obstruct data subjects in exercising their rights or receiving the services? yes **no**

Other reasons that pose a high risk for the rights and freedoms of natural persons: none

Is high risk for the rights and freedoms of natural persons probable (the condition is met if at least 2 factors apply, or is there any other reason to justify the high risk)? no

Examination of risks:

Risk value (score) = Impact of occurrence (score) x probability of occurrence (score)

Risk classification:

Risk value 1-12 points: low-risk

Risk value 13-19 points: medium-risk

Risk value 20-25 points: high-risk

Event	*Impact*	*Probability*	*Risk value*	*Recommended measure*	*Decision*

	1-5	*1-5*	*1-25*		
unauthorized access	2	2	4	increased control of the implementation of security requirements	
undesirable change	1	1	1	no recommended change	
loss of data	4	3	12	IT review	
fire damage	5	1	5	no recommended change	
water damage	5	1	5	no recommended change	
IT network error	3	4	12	periodic review	

Risk management measures:

- regulation of security measures
- adherence to the regulations
- teaching employees, which promotes more knowledgeable data management and procedures

Evaluation and commenting on impact assessment:

Deputy Senior Director:

The use of the electronic surveillance system is essential for the purposes of property protection, as the company manages a significant amount of state assets during the course of performing its public tasks. The system was developed by a reliable contractor awarded the project as part of a public procurement procedure. In line with our administrative obligations, we have prepared the Privacy Policy applicable to the persons who enter the area and to our public servants and employees, and we attribute great importance to applying and ensuring other comply with the provisions of the Privacy Policy. The impact assessment has provided the reassuring results that the risks in data processing are low.

_____

Dr. Virág Főző

Deputy Senior Director

IT Director:

During data processing, we comply with the applicable IT security requirements and regulations. The data are protected with physical and logical systems. Physical security is ensured by the lockable, fire and waterproof server room that can be accessed only by IT Department employees and the Security Manager. This aims to guarantee that data will not be lost or changed, and that no unauthorised persons may access those. Only IT Department employees, the Technical Director, the Facility Management Department Head, the Security Manager, and the persons authorised by them in writing are entitled to inspect and restrict access to the data.

_____

Kolos Kováts

IT Department Head

Security Manager:

The data controller selected the company that deals with property protection by way of a public procurement procedure conducted in line with the rules of Act CXLIII of 2015 on Public Procurement (hereinafter: Public Procurement Act); the company provides property protection, reception, cash security, cash transport, and patrol services at the Hungarian State Opera's venues and sites. The Technical Directorate of the Hungarian State Opera, as data controller, and T.O.M. Controll 2001 Zrt., which deals with static force protection, as data processor, cooperate in the course of performing property protection tasks. The properly trained security guards and reception service employees employed by the data processor fully comply with all provisions of the Privacy Policy when performing their tasks, which the Security Manager and the managers of the data processor continuously monitor to ensure that no abuses can take place involving personal data.

_____

Gábor Vágó

Technical Director

Annex 5

DATA BREACH RECORDS

NAME OF CONTROLLER:	The Hungarian State Opera
REGISTERED SEAT:	1061 Budapest, Andrássy út 22.
REGISTRY ID:	309435
TELEPHONE NUMBER:	0618147444
EMAIL ADDRESS:	dpo@opera.hu
WEBSITE:	www.opera.hu
REPRESENTATIVE NAME:	Szilveszter Ókovács, General Director

DATA BREACH RECORDS

SERIAL	DATE OF BREACH:	NAME AND ATTRIBUTES OF THE BREACH:	SPHERE OF DATA SUBJECTS:	THE PERSONAL DATA CONCERNED:	THE EFFECTS OF THE BREACH:	THE MEASURES IMPLEMENTED TO COUNTER THE BREACH:	OTHER DATA:
1/2018	2018-06-01	damages to the video recording prior to the expiry of the retention period	images of the people who enter and stay in the area, as recorded by the video surveillance system	video recording of the private persons who were in the area between 11:00 am on 29 May 2018 and 6:00 pm on 29 May 2018	damages to the data, data l	Report to the supervisory authority Hungarian National Authority for Data Protection and Freedom of Information (NAIH) due to the high risk level. Inspection of the reasons for the breach and warning the employee responsible.	SAMPLE!!!
2/2018	2018-06-02	the video recordings were disclosed to the public	Stephen Sample and Ernest	video recording of the data s	Unauthorised access, discl	The supervisory authority (Hungarian National Authority for Data Protection and Freedom of Information - NAIH) was informed	SAMPLE!!!

Annex 6:

~ Records of inspections of electronic surveillance data ~

SAMPLE

<table>
<tr><td>Minutes no.:</td><td>1/2020.</td></tr>
<tr><td>Prepared:</td><td>8 March 2020</td></tr>
<tr><td>Venue:</td><td>Rehearsal Studio at 1066 Budapest, Jókai utca 4.</td></tr>
<tr><td>Recording data:</td><td>The recordings of the camera facing the hallway in front of the entrance, made between 10:00 am and 12:30 pm on 3 March 2020</td></tr>
<tr><td>Start and end dates of viewing the recording:</td><td>8 March 2020 10:00 am to 2:00 pm</td></tr>
<tr><td rowspan="2">The following persons are present
(name, position):</td><td>Kolos Kovács, IT Department Head</td></tr>
<tr><td>Gábor Vágó, Technical Director</td></tr>
<tr><td colspan="2">A description of the circumstance giving rise to the viewing:
Between 10:00 am and 12:30 pm on 3 March 2020, unknown perpetrators stole a laptop and smartphone from the Ferencsik Room containing valuable and sensitive data. The rehearsal studio door was unlocked and there were no signs of forced entry at the window, so it can be assumed that the theft was carried out by a person who accessed the rehearsal studio through its only door. To investigate the event, the above persons are reviewing the video recordings made at the above time period.</td></tr>
<tr><td colspan="2">The conclusions drawn during the viewing:
The recording viewed clearly shows that a hooded, 190 cm tall man slipped into the rehearsal studio at 11:24 am on 3 March 2020 and walked out towards the main entrance at 11:28 am, carrying the laptop and smartphone.</td></tr>
<tr><td colspan="2">Dated as above</td></tr>
<tr><td>Keeper of the minutes:

signature:

_____</td><td>Names and signatures of those present:

_____

_____</td></tr>
<tr><td colspan="2">The recorded images and other personal data (including the minutes) have to be promptly submitted to the court or authority if requested by the court, prosecutor’s office, investigating authority, the body conducting a preparation process, or other authority. If no such request is submitted within thirty days of the omission of erasure having been requested, the recorded image or other personal data (also including the minutes) have to be erased or destroyed, unless the 30-day retention period has not yet expired.</td></tr>
</table>