Bvd. Corneliu Coposu, nr.2, 550245 Sibiu, România Tel.: +4 0269 210 092 Fax: +4 0269 210 532 CIF 4556190 www.tnrs.ro facebook.com/TNRSS

Annex to Decision No.93 of 9 November 2018

REGULATION ON

THE PROTECTION OF PERSONAL DATA

"RADU STANCA" NATIONAL THEATRE SIBIU

SUMMARY:

CHAPTER 1 GENERAL PROVISIONS 5

1. 1. Subject-matter and objectives 5

1.2. Scope 5

1.3. Terminology and definitions 5

1.4. 2.1 Reference documents 10

CHAPTER 2. PRINCIPLES RELATING TO PROCESSING OF PERSONAL DATA 10

2.1. Lawfulness, fairness and transparency 8

2.2. Purpose limitation 9

2.3. Minimization/Data minimisation 9

2.4. Information accuracy 9

2.5. Storage limitation 9

2.6. Integrity and confidentiality 9

2.7. Responsibility 9

CHAPTER 3. LAWFULNESS OF PERSONAL DATA PROCESSING 10

CHAPTER 4 DATA SUBJECT'S CONSENT AND CONDITIONS FOR CONSENT 11

CHAPTER 5. SPECIAL RULES ON PERSONAL DATA PROCESSING 12

5.1. Processing of special categories of personal data 12

5.2. Processing of personal data with a general identification function . 13

5.3. Processing of personal data relating to criminal convictions and offences 14

5.4. Processing which does not require identification 14

5.5. Processing of personal data by video surveillance systems 14

5.6. Processing in the context of employment 15

5.7. Personal data processing for promotional (marketing) purposes ... 15

CHAPTER 6 RIGHTS OF THE DATA SUBJECT IN THE CONTEXT OF PERSONAL DATA PROCESSING 20

6.1. Transparent information, communication and modalities for the exercise of the rights of the data subject 20

6.2. Right to be informed 21

6.2.1. Information to be provided where personal data are directly collected from the data subject. 21

6.2.2. Information to be provided where personal data have not been obtained from the data subject 22

6.2.3. Information to be provided to data subjects within the context of TNRS specific activities 19

6.3. Right of access by the data subject 21

6.4. Right to rectification 22
6.5. Right to erasure ("right to be forgotten") 22
6.6. Right to restriction of processing 22
6.7. Notification obligation regarding rectification or erasure of personal data or restriction of processing 23
6.8. Right to data portability 23
6.9. Right to object and automated individual decision-making 30
CHAPTER 7 RESTRICTIONS 24
CHAPTER 8 CONTROLLER AND PROCESSOR 31
8.1. Responsibility of the controller 31
8.2. Data protection by design and by default 28
8.3. Processor 29
8.5. Records of processing activities 30
8.6. Cooperation with the Supervisory Authority 31
8.7. Appropriate technical and organizational measures for personal data protection 31
8.7.1. General aspects regarding the security of processing 39
8.7.2. General aspects regarding the security of processing 40
8.7.3. Personal data mapping 41
8.7.4. GDPR rules for database management 33
8.8. Notification of a personal data breach to the supervisory authority 42
8.9. Communication of a personal data breach to the data subject 44
CHAPTER 9 DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION 44
9.1. Data protection impact assessment 44
9.2. Pre-consultation of the Supervisory Authority 46
CHPATER 10 DATA PROTECTION OFFICER 37
10.1. Assignment of responsibilities/tasks to the Data Protection Officer 37
10.2. TNRS Responsibilities in relation to the Data Protection Officer 38
CHAPTER 11 TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS 39
CHAPTER 12 SPECIFIC REMEDIES, LIABILITY AND PENALTIES 50
12.1. Right to lodge a complaint with a supervisory authority 50
12.2. Right to an effective judicial remedy against a supervisory authority 50
12.3. Right to an effective judicial remedy against a controller or controller's processor 50

12.4. Right to compensation and liability of the controller or processor . 51
12.5. General conditions for imposing administrative fines 51
CHAPTER 13 RESPONSIBILITIES WITHIN TNRS 53
CHPATER 14 TNRS EMPLOYEES' COMPLIACE COMMITMENT TO THE SPECIFIC LEGISLATION AND TNRS PERSONAL DATA PROTECTION REGULATION 57
CHAPTER 15 TRAINING 58
CHAPTER 16 FINAL PROVISIONS 58
Annex 1 Information note on personal data protection for prospective employees
Annex 2 Information note on personal data protection for employees
Annex 3 Information on personal data processing by video surveillance systems
Annex 4 Compliance commitment
Annex 5 Provisions on personal data protection - Contract adhesion
Annex 6 Provisions on personal data protection - Contracts
Annex 7 Website terms and conditions
Annex 8 GDPR consent for Newsletter
Annex 9 GDPR consent for visitors and acquisitions
Annex 10 Access request
Annex 11 Rectification request
Annex 12 Erasure request
Annex 13 Personal data identification form
Annex 14 GDPR provisions - General conditions
Annex 15 Information/Consent statement for direct marketing purposes within the context of personal data processing
Annex 16 Processor - Contracts

CHAPTER 1 GENERAL PROVISIONS

1. 1. Subject-matter and objectives

1.1.1. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and the free movement thereof;

1.1.2. This Regulation protects the fundamental rights and freedoms of natural persons and in particular their right to the protection of their personal data;

1.1.3. Exercising the rights provided for in this Regulation may only be restricted in the cases expressly covered by and exhaustively listed in the law.

1.1.4. The free movement of personal data within the European Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.

1.2. Scope

1.2.1. This regulation shall apply to all TNRS employees with duties involving personal data processing and/or, as the case may be, to TNRS processors.

1.2.2. This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

1.3. Terminology and definitions

For the purposes of this Regulation:

1. "***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;

2. "***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* - gathering, putting together or receipt of personal data by any legal means and from any source;
- *recording* - recording of personal data in an automated or non-automated filing system, which may be a register, automated file, database or any form of filing, whether organized, structured or *ad hoc*, or in a text, data set or document, regardless of the way the data is recorded;
- *organizing* - ordering, structuring or systematizing personal data, in accordance with pre-set criteria, according to the legal responsibilities of the controller, in order to increase the efficiency/optimize this latter's processing activities;
- *storage* - preservation of personal data collected in any type of medium, including backup;
- *adaptation* - processing of initially-collected personal data in accordance with the pre-set criteria and with the purpose for which the personal data were collected;
- *alteration* - updating, filling in, changing, correcting or restoring personal data in order to maintain the accuracy, reality and timeliness characteristics;

- retrieval - removal of a part of the specific category of personal data for the purpose of using it separately and distinctly as compared to the original processing;
- *consultation* - examining, viewing, querying or investigating personal data, without limitation thereto, for the purpose of carrying out a subsequent processing operation or set of operations;
- *use* - using personal data, in whole or in part, by and within the controller, controller's or recipient's processors, as the case may be, including printing, copying, multiplication, scanning or any other similar processes;
- *disclosure* - making personal data available to third parties by means of communication transmission, dissemination or otherwise making available;
- *joining* - adding, adjoining or attaching personal data to the existing ones that they do not modify;
- *combination/alignment* - merging, uniting or assembling initially separated personal data into a new form based on pre-set criteria for specifically determined purposes;
- *blocking* - interruption of personal data processing;
- *restriction* - marking of stored personal data with the aim of limiting their processing in the future;
- *erasure* - deletion or removal, in whole or in part, of personal data from the records or registrations upon expiration of the retention period, when reaching the purpose for which they were introduced, invalidity, non-existence, inaccuracy;
- *transformation* - personal data processing with the purpose of anonymizing or using it exclusively for statistical purposes;
- *destruction* - bringing the physical medium on which the personal data were processed. into an unusable, definitive and irrecoverable state, as provided by law, by using mechanical or thermal means.

3. "***Profiling***" means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

4. "***Pseudonymisation/anonymous data***" means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

5. "***Filing system***" means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

6. "***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 a legal act or based on a legal act, the controller is the natural or legal person, governed by public law or by private law, who is nominated as a controller by such a legal act or based on such a legal act. *For the purposes of this Regulation, the Controller shall be TNRS, with all the functional entities/organizational structures - directorates, departments, services, offices, compartments, boards, committees, etc., if they establish the purposes for which and the means by which personal data is to be processed*

7. "***Person empowered by the controller/processor***" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

8. "***Recipient***" means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. Nevertheless, the public authorities to which personal data may be communicated within the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

9. "***Third party***" means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

10. "Consent" of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

11. "***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;

12. "Genetic data" means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

13. "Biometric data" means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

14. "Data concerning health" means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

15. "***Enterprise***" means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;

16. "***Group of undertakings***" means a controlling undertaking and its controlled undertakings;

17. "Binding corporate rules" means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity;

18. "Supervisory authority concerned/NSAPDP" means the National Supervisory Authority for Personal Data Processing;

19. "Personal Numeric Code (CNP)" means a significant number that uniquely identifies a natural person as a tool for verifying his or her marital status and identification thereof in certain computer systems by authorized persons;

20. *"Personal data as an identifier of general application (special data)"* means numbers identifying a natural person in certain filing systems that are of general application, such as: personal numeric code, serial number and identity card number, passport number, driving license number, social or health insurance number;

21. "User" means any person acting under the authority of the controller, of the processor or of the representative, with a recognized right of access to personal data bases; *has the quality of user of the personal data, the Controller's personnel - TNRS or this latter's processor, whose duties include personal data processing operations.*

22. "Data protection officer" means a person within the TNRS with specific tasks/responsibilities regarding the proper functioning of the personal data protection system in accordance with the GDPR provisions as well as the development, implementation and monitoring of compliance with the provisions of this Regulation.

1.4. 2.1 Reference documents

- 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 (GDPR);

Law No. 190 of 18 July 2018 on the measures for the application of Regulation (EU)2016/679of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

- Domestic law applicable in the field of personal data protection;
- ORDINANCE No. 21 of January 31, 2007 on institutions and companies operating in the area of performing arts or concerts and the performance of artistic agency activities;
- TNRS rules of organization and operation
- Internal rules and procedures.

CHAPTER 2. PRINCIPLES RELATING TO PROCESSING OF PERSONAL DATA

2.1. Lawfulness, fairness and transparency - an essential principle, closely associated with fundamental human rights. Personal data must be processed ***"lawfully, fairly and transparently in relation to the data subject";***

2.2. **"Purpose limitation"** - Personal data shall be collected ***for specified, explicit and legitimate purposes***, and further processing shall not deviate from these purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should not be considered incompatible with the initial purpose;

2.3. **Minimization/Data minimisation** - any personal data collection operation shall be thoroughly considered prior to the effective collection of such data and this latter should be ***adequate, relevant and limited*** to what is strictly necessary for the purposes for which they are processed;

2.4. Information accuracy - personal data must be accurate and, where necessary, kept up to date; every reasonable step must be taken by controllers to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

2.5. **Storage limitation** - data must be kept as long as it is required for the purpose of the assumed processing. Longer storage periods are exceptions associated with processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) of GDPR subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject;

2.6. **Integrity and confidentiality** - personal data must be processed under the most appropriate security conditions, including "protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures".

Failure to comply with this principle may directly lead to breaches of security and confidentiality and, implicitly, to the extremely severe penalties as referred to in GDPR;

2.7. **Responsibility - *The controller shall be responsible for ensuring compliance with GDPR principles and demonstrating this compliance.*** Not only does GDPR require compliance with the GDPR principles - for example by documenting decisions taken regarding a processing activity, but also being able to demonstrate such compliance (accountability) at any time.

Consequently:

- *Any processing of personal data should be lawful and fair;*
- *It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed;*
- *The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used; this principle concerns, in particular information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure a fair and transparent processing in respect of the natural persons*

concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed;

- *Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing;*
- *In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data;*
- *The personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed. This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum;*
- *Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means;*
- *The controller should set time limits for erasure or for a periodic review. The controller shall take every reasonable to ensure that personal data which are inaccurate are rectified or deleted;*
- *Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or use of personal data and the equipment used for the processing.*

CHAPTER 3. LAWFULNESS OF PERSONAL DATA PROCESSING

Processing shall be lawful only if and to the extent that at least one of the following applies:

a) ***the data subject has given consent to the processing of his or her personal data for one or more specific purposes;***

b) ***processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;***

c) ***processing is necessary for compliance with a legal obligation to which the controller is subject;***

d) ***processing is necessary in order to protect the vital interests of the data subject or of another natural person;***

e) ***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 controller;***

f) ***processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.***

Note: *"The legitimate interests of a controller", including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their*

relationship with the controller. Such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller. The processing of personal data strictly necessary for the purposes of preventing fraud may also constitute a legitimate interest of the data controller concerned.

CHAPTER 4 DATA SUBJECT'S CONSENT AND CONDITIONS FOR CONSENT

4.1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented expressly, clearly, freely and in an informed manner to the processing of his or her personal data.

4.2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.

4.3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

4.4. When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

4.5. ***Within TNRS, as a Personal data controller, the data subjects' consent shall be given:***

- as part of the personnel recruitment/selection process;
- upon the conclusion of contracts with business partners, only in the case where the personal data is processed for direct marketing purposes (provision of information about TNRS services, events and exhibitions;
- when subscribing to newsletters (provision of information on ***TNRS*** services, events and exhibitions;
- when setting up an account on TNRS websites to access specific services, invite specialists to attend festivals, the performing arts market, exhibitions and such other events (for direct marketing purposes).

4.6. During the personnel recruitment/selection process, the Human Resources Specialist - TNRS shall request the consent of the prospective employee by having this latter sign an *Information Note* stating that he or she has been informed about the processing of personal data within ***TNRS***, as well as about their rights under the specific legislation. The Information Notes shall be kept separately in the records of the Human Resources Specialist.

4.7. Should the TNRS management decide to process for direct marketing purposes, i.e. provide contractual partners with information about ***TNRS*** services, events and exhibitions etc.,

the functional entities/contract managers/persons responsible for the contract shall obtain for the aforementioned purpose the consent of the data subject concerned by ticking a dedicated box in the contract. Lack of consent leads to the impossibility of processing for direct marketing purposes.

4.8. In the case of subscription to newsletters, the data subject's consent is given by ticking a dedicated box in the relevant website section, the person being informed about personal data protection issues.

4.9. If setting up an account on TNRS websites for the purchase of services/online payment of fees, access to specific services, as well as sending online invitations to specialised visitors in view of their participation in the festival, performing arts market and other events, etc., the data subject's consent is given by ticking dedicated boxes in the relevant website section, the data subject being informed about personal data protection issues.

4.10. *The functional entities/contract managers/persons responsible for the contract as well as those responsible for direct marketing operations (including IT-related services) will necessarily take into account the consent given by the data subject in order to avoid situations of non-compliance with the legal provisions on personal data protection.*

4.11. If personal data processing is based on consent, processing a child's data is legal only if he or she is at least 16 years of age. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology. These provisions shall not affect the general contract law of EU Member States such as the rules on the validity, formation or effect of a contract in relation to a child.

CHAPTER 5. SPECIAL RULES ON PERSONAL DATA PROCESSING

5.1. Processing of special categories of personal data

5.1.1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation **shall be prohibited**.

5.1.2. The aforementioned provisions shall not apply in the following situations:

a) *the data subject has given explicit consent to the processing of those personal data* for one or more specified purposes, except where Union or domestic law provide that the prohibition referred to above may not be lifted by the data subject;

b) *processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law* in so far as it is authorised by Union or domestic law or a collective agreement pursuant to domestic law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

c) *processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;*

d) *processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;*

e) *processing relates to personal data which are manifestly made public by the data subject;*

f) *processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;*

g) *processing is necessary for reasons of substantial public interest, on the basis of Union or domestic law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;*

h) *processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or domestic law or pursuant to contract with a health professional and subject to the conditions and safeguards provided by law;* personal data may be processed for the above-mentioned purposes when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or domestic law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or domestic law or rules established by national competent bodies.

i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or domestic law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy; or

j) *processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes,* on the basis of Union or domestic law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

5.2. Processing of personal data with a general identification function

Personal data with a general identification function (Personal Numerical Code - CNP, serial number and ID/passport number, etc.) shall be processed only where the identity of the data subjects must be established, and such processing is expressly provided for by a legal provision.

The domestic law may further determine the specific conditions for the processing of a national identification number or any other identifier of general application. In that case, the national identification number or any other identifier of general application shall be used only under appropriate safeguards for the rights and freedoms of the data subject.

5.3. Processing of personal data relating to criminal convictions and offences

Processing of personal data relating to criminal convictions and offences or related security measures shall be carried out only under the control of official authority or when the processing is authorised by Union or domestic law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.

5.4. Processing which does not require identification

5.4.1. If the purposes for which the TNRS (controller) processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with the specific legislation.

5.4.2. Where, in the above-mentioned cases, the controller is able to demonstrate that it is not in a position to identify the data subject, the controller shall inform the data subject accordingly, if possible. In such cases, the legal provisions on the right of access, rectification, erasure, restriction of processing, the right to data portability shall not apply except where the data subject, for the purpose of exercising his or her rights mentioned above, provides additional information enabling his or her identification.

5.5. Processing of personal data by video surveillance systems

TNRS, through video surveillance systems, processes personal data, such as image and other information permitting the identification of the data subjects.

Images of identified or identifiable persons processed by video surveillance systems, constitute personal data:

a) even if they are not associated with the data subject's identification data or

b) even if they do not contain the image of the filmed person, but other information likely to lead to his or her identification (e.g. vehicle registration number)

The purpose of processing personal data is to: monitor/ensure the security of individuals, premises and/or private goods, prevent and combat crime, fulfil legal obligations and achieve legitimate interests.

Personal data processing by video surveillance systems is to be carried out only by persons authorized by **TNRS**.

The registered information is to be used by **TNRS** and may only be communicated to the following recipients: the data subject, the legal representatives/proxies of the data subject, **TNRS** authorized representatives, criminal prosecution/investigation bodies, law courts, according to the provisions of the domestic and community legislation applicable to the activity carried out by **TNRS**.

The storage period for the data obtained by video surveillance systems is 30 days, except where expressly regulated by law or in duly justified cases. Upon expiration of the term, the records shall be destroyed or deleted.

The data subjects concerned, namely the employees, clients/prospective clients, the visitors and other persons entering the ***TNRS headquarters - a real estate under TNRS management, 2 Corneliu Coposu Blvd., Sibiu, Ticket Agency - a real estate under TNRS management - 17 Nicolae Bălcescu Blvd., Sibiu, Fabrica de Cultură- a real estate over which TNRS has a usage right - 1- 3 Triajului Street, Sibiu*** are informed on personal data processing by video surveillance systems.

Related information as well as signage as to the existence of the video surveillance system shall be displayed in the locations where CCTV video surveillance cameras are placed. *The security staff of the Administrative Service shall regularly check the physical state of the aforementioned information and signage and shall be responsible for the security and confidentiality of the personal data stored in the video surveillance/monitoring system.*

5.6. Processing in the context of employment

5.6.1. Member States may, by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the context of employment, in particular for the purposes of recruitment, the fulfilment of the clauses of the employment contract, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, protection of employer's or customer's property and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.

5.6.2. Those rules shall include suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights, with particular regard to the transparency of processing, the transfer of personal data within a group of undertakings, or a group of enterprises engaged in a joint economic activity and monitoring systems at the work place.

5.7. Personal data processing for promotional (marketing) purposes

Personal data provided by the data subjects (such as the name and surname, e-mail address, fax number, mobile/landline phone number) may be processed by ***TNRS*** only based on the previously and freely given consent in an express, unambiguous and informed manner (***Annex 15***), in certain cases, in compliance with their rights, in particular the right to information and objection, for the following purposes: marketing (including direct marketing), contests, advertising lotteries, commercial advertising for services provided by **TNRS**, including those developed together with a **TNRS** partner, by any means of communication, including electronic communication services. The personal data provided by the data subjects may be used for promotional (marketing) purposes and for the products or services of other **TNRS** partners, while respecting the data subjects' rights.

The data subjects may exercise their right to prevent such processing by ticking the appropriate boxes in the forms/documents used to collect personal data.
Whatever the case may be, if the data subject would like personal data not to be processed by **TNRS**, he or she may expressly request that any processing of data by **TNRS** be terminated. At the same time, when the data subject no longer wants to receive newsletters or information materials from **TNRS**, he or she can unsubscribe using the "*Dezabonare*" or "Unsubscribe" button.

CHAPTER 6 RIGHTS OF THE DATA SUBJECT IN THE CONTEXT OF PERSONAL DATA PROCESSING

6.1. Transparent information, communication and modalities for the exercise of the rights of the data subject

6.1.1. TNRS (THE CONTROLLER) shall take appropriate measures to provide the data subject with any legal information requested as well as any notifications and communications (when exercising the rights he or she enjoys under the law) relating to processing in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

6.1.2. TNRS facilitates the exercise of data subject rights.

6.1.3. ***TNRS shall provide the data subject with information on action taken based on a request through which he or she exercises his or her rights under the law without undue delay and in any event within one month of receipt of the request.*** That period may be extended by two further months where necessary, taking into account the complexity and number of the requests.

6.1.4. TNRS shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

6.1.5. If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

6.1.6. The information provided under the specific law as well as any communication and any measures taken based on the exercise of the rights enjoyed by the data subject under the law, <u>are offered free of charge.</u> <u>Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either:</u>

a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or

b) refuse to act on the request.

In such cases, the controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

6.1.7. Where the controller has reasonable doubts concerning the identity of the natural person making the request through which the data subject exercises his or her rights under the law, the operator may request the provision of additional information necessary to confirm the identity of the data subject.

6.1.8. The information to be provided to data subjects pursuant to specific legislation may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing. Where the icons are presented electronically, they shall be machine-readable.

6.1.9. *In order to exercise the rights under the specific legislation and this Regulation, the data subjects may contact the TNRS Data Protection Officer by sending a written request, dated and signed at the e-mail address: administrator@sibfest.ro or at the following mailing address: TNRS,* ***the TNRS building, str. Bd. Corneliu Coposu nr.2 Sibiu,*** *TNRS may, if necessary, request the data subject to provide additional information in order to establish his or her identity.*

6.2. Right to be informed

6.2.1. Information to be provided where personal data are directly collected from the data subject.

6.2.1.1. Where personal data relating to a data subject are collected from this latter, TNRS shall, at the time when personal data are obtained, provide the data subject with the following information:

a) the identity and the contact details of the controller and, where applicable, of the controller's representative;

b) the contact details of the data protection officer, where applicable;

c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

d) the legitimate interests pursued by the operator or a third party, as the case may be;

e) the recipients or categories of recipients of the personal data;

f) where applicable, that the controller intends to transfer personal data outside the EU Area or outside the European Economic Area and the existence or absence of an adequacy decision by the Commission regarding the protection level or, reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available.

6.2.1.2. *In addition* to the above-mentioned information, the controller shall, at the time when personal data are obtained, provide the data subject with *the following further information* necessary to ensure fair and transparent processing:

a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;

c) where processing is based on the data subject's consent, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

d) the right to lodge a complaint with a supervisory authority;

e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

f) the existence of automated decision-making, including profiling, and, at least, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

6.2.1.3. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information;

6.2.1.4. The aforementioned provisions shall not apply where and insofar as the data subject already has the information.

6.2.2. Information to be provided where personal data have not been obtained from the data subject

6.2.2.1 Where personal data have not been obtained from the data subject, TNRS shall provide the data subject with the following information:

a) the identity and the contact details of the controller and, where applicable, of the controller's representative;

b) the contact details of the data protection officer, where applicable;

c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

d) the categories of personal data concerned;

e) the recipients or categories of recipients of the personal data, if any;

f) where applicable, that the controller intends to transfer personal data outside the EU Area and outside the European Economic Area and the existence or absence of an adequacy decision by the Commission regarding the protection level or, reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available.

6.2.2.2. *In addition to the aforementioned information*, the controller shall provide the data subject with *the following information necessary* to ensure fair and transparent processing in respect of the data subject:

a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

b) the legitimate interests pursued by the operator or a third party, as the case may be;

c) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability;

d) where processing is based on the data subject's consent, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

e) the right to lodge a complaint with a supervisory authority;

f) from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;

g) the existence of automated decision-making, including profiling, and, at least, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

6.2.2.3. The controller provides the aforementioned information:

a) within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed;

b) if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or

c) if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

6.2.2.4. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information.

6.2.2.5 The preceding provisions shall not apply where and insofar as:

a) the data subject already has the information;

b) the provision of such information proves to be impossible or would involve disproportionate efforts, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and guarantees laid down by law; or insofar as the obligation to provide information is likely to render impossible or seriously impair the achievement of the objectives of the processing. In such cases, the controller shall take appropriate measures to protect the rights, freedoms and legitimate interests of the data subject, including making the information publicly available;

c) obtaining or disclosure is expressly laid down by Union or domestic law to which the controller is subject and which provides appropriate measure to protect the data subject's legitimate interests; or

d) where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or domestic law, including a statutory obligation of secrecy.

6.2.3. Information to be provided to data subjects within the context of TNRS specific activities

Within the context of performance of their duties as laid down by law and the performance of TNRS current activity, including the performance of the employment relationship, commercial/contractual activity and/or participation in tours, festivals and/or other specialized events organized within the premises of TNRS and in the context of fulfilment of legal obligations**, the provision of information to the data subjects may be done as follows:**

- During the personnel recruitment/selection process, the Human Resources Specialist - TNRS shall provide the prospective employee with an *Information Note* that he or she shall read and sign and by which he or she declares having been informed about the processing of personal data by TNRS, as well as about the rights they enjoy under the specific legislation. The Information Notes shall be kept separately in the records of the Human Resources Specialist. *A template of the Information Note for the potential employee is set out in* ***Annex 1;***
- Within the context of performance of their work, the Human Resources Specialist - TNRS shall each TNRS employee with an *Information Note* that he or she shall read and sign and through which he or she declares having been informed about the processing of personal data by TNRS, as well as about the rights they enjoy under the specific legislation. The Information Notes shall be kept separately in the records of the Human Resources Specialist. *A template of the Information Note for employees is set out in* ***Annex 2;***
- The data subjects concerned, namely the employees, the clients/potential clients, the visitors and other persons entering the ***TNRS headquarters - an immovable property managed by TNRS, 2 Corneliu Coposu Blvd., Sibiu, Theatre Agency - an immovable property managed by TNRS - 17 Nicolae Bălcescu Blvd., Sibiu, Fabrica de Cultură- a real estate over which TNRS has a usage right - 1-3 Triajului Street, Sibiu,*** whose data are processed through video surveillance systems are informed in this respect by means of *Information Notes. The template of the Information Note on data processing through video surveillance systems is set out in* ***Annex 3.*** *Related information as well as signage as to the existence of the video surveillance system shall be displayed in the locations where CCTV video surveillance cameras are placed by the Administrative Department. The security staff within the Administrative Department shall regularly check the physical state of the aforementioned information panels and signage and shall be responsible for the security and confidentiality of the personal data stored in the video surveillance/monitoring system.*
- Within the performance of the commercial/contractual activity and/or participation in tours, festivals and/or other specialized events organized within the **premises of TNRS** 2 **Corneliu Coposu Blvd., Sibiu, the provision of information to the data subject is achieved by:**
  - General and Technical Conditions of Participation of TNRS, which include provisions on the protection of personal data ***(Annex 14);***
  - The form "Contract Adhesion", which includes the provisions on personal data protection ***(Annex 5);***

- The contractual documents concluded by TNRS, which include provisions on personal data protection ***(Annex 6);***
- The Terms and Conditions specific to TNRS websites, which include provisions on personal data protection ***(Annex 7);***
- TNRS websites, in case of newsletter subscription case, setting up an account to purchase services/pay the tariff online, access specific services as well in the case of online invitations sent to specialists to invite them to participate in festivals, tours and such other events etc.

TNRS contractual partners will have the responsibility/obligation to insert in the contracts concluded and managed by them specific clauses regarding personal data protection and/or the observance of the General and Technical Conditions of Participation.

The content of the Information Notes, contractual clauses, and other information tools relating to the protection of personal data is established/updated on the basis of specific legislation by the Data Protection Officer of TNRS and approved in advance by the TNRS management.

6.3. Right of access by the data subject

6.3.1. The data subject shall have the right to obtain from the controller confirmation 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 following information:

a) the purposes of the processing;

b) the categories of personal data concerned;

c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

d) where possible, the envisaged period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

f) the right to lodge a complaint with a supervisory authority;

g) 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, including profiling, and, at least, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

6.3.2. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards provided by law relating to the transfer.

6.3.3. The controller shall provide a copy of the personal data undergoing processing. 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.

6.3.4. The right to obtain the copy referred to above shall not adversely affect the rights and freedoms of others.

In order to exercise the right, the data subject may use the application form provided in Annex 10.

6.4. Right to rectification

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. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

In order to exercise the right, the data subject may use the application form provided in Annex 11.

6.5. Right to erasure ("right to be forgotten")

6.5.1. 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 have the obligation to erase personal data without undue delay where one of the following grounds applies:

a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

b) the data subject withdraws consent on which the processing is based and there is no other legal ground for the processing;

c) the data subject objects to the processing and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing in the case of processing for direct marketing purposes;

d) the personal data have been unlawfully processed;

e) 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;

f) the personal data have been collected in relation to the offer of information society services referred to in the specific law.

6.5.2. The preceding paragraphs shall not apply to the extent that processing is necessary:

a) for exercising the right of freedom of expression and information;

b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

c) for reasons of public interest in the area of public health;

d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in so far as the right to erasure is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

e) for the establishment, exercise or defence of legal claims.

In order to exercise the right, the data subject may use the application form provided in Annex 12.

6.6. Right to restriction of processing

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

a) 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;

b) the processing is unlawful, and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

c) 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 defence of legal claims; or

d) the data subject has objected to processing pending the verification whether the legitimate grounds of the controller override those of the data subject.

6.6.2. Where processing has been restricted under the preceding provisions, 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.

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

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

The 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.

6.8. Right to data portability

6.8.1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

a) processing is based on consent or contract; and

b) the processing is carried out by automated means.

6.8.2. In exercising his or her right to data portability, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

6.8.3. Exercising the right to data portability shall not prejudice to the right to data erasure. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

6.8.4. The right referred to data portability shall not adversely affect the rights and freedoms of others.

6.9. Right to object and automated individual decision-making

6.9.1. Right to object

6.9.1.1. The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her, including profiling. 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 defence of legal claims.

6.9.1.2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

6.9.1.3 Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

6.9.1.4. At the latest at the time of the first communication with the data subject, the right to object referred to shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.

6.9.1.5. Where personal data are processed for scientific or historical research purposes or statistical purposes, the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

6.9.2. Automated decision-making, including profiling

6.9.2.1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

6.9.2.2. The preceding provisions shall not apply if the decision:

a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;

b) is authorised by Union or Member State law to which the controller is subject, and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

c) is based on the data subject's explicit consent.

6.9.2.3. In the cases where decision is necessary for the entering or performance of a contract between the data subject and a controller, or when the data subject has given his or her explicit consent, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

6.9.2.4. The decisions referred to above are not based on special categories of personal data, with the exceptions provided by law (e.g. the data subject has given explicit consent) and where suitable measures to safeguard the data subject's rights, freedoms and legitimate interests are in place.

CHAPTER 7 RESTRICTIONS

The specific law to which the data controller or processor is subject may restrict the scope of the obligations and rights provided for in the current legislation in so far as its provisions correspond to the rights and obligations referred to above, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:

a) national security;

b) defence;

c) public security;

d) 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;

e) other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters, public health and social security;

f) the protection of judicial independence and judicial proceedings;

g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;

h) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority;

i) the protection of the data subject or the rights and freedoms of others;

j) the enforcement of civil law claims.

CHAPTER 8 CONTROLLER AND PROCESSOR

8.1. Responsibility of the controller

8.1.1. Taking into account the nature, scope, context and purposes of processing, costs of implementation as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, ***TNRS shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the specific law***.

Also, the technical and organizational measures adopted by TNRS are necessary to protect personal data against accidental or unlawful destruction, loss, modification, unauthorized disclosure or access. Those measures shall be reviewed and updated where necessary.

In order to meet the legal requirements specific to the protection of personal data, TNRS shall implement technical and organizational measures targeting different directions of action, such as: assigning/setting responsibilities for the Data Protection Officer, assigning/responsibilities for employees processing personal data, data protection, drafting the data protection rules, adapting the activities of the organization to specific legal requirements, developing/implementing appropriate IT policies/procedures for personal data security, staff training, compliance monitoring, etc.

8.1.2. Technical and organizational measures ***include the implementation by TNRS of appropriate IT policies/procedures for personal data protection/security.***

The TNRS IT Office has the responsibility/obligation to develop/update and implement appropriate policies/procedures to ensure personal data protection/security.

8.1.3. ***<u>In addition</u>*** to the above-mentioned measures, in order to ensure an appropriate level of personal data protection/security, ***<u>organizational measures and rules shall be adopted/established</u>*** at the level of TNRS, ***<u>such as:</u>***

- *Installation of video surveillance systems and intrusion systems;*
- *Permanent monitoring and intervention in case of alarm by specialized/authorized personnel;*
- *All documents containing personal data shall be registered and observe the rules of storage, processing, multiplication, transport, destruction and archiving laid down by the National Archives Law, domestic and international legislation on personal data protection, and by the internal procedures;*
- *TNRS personnel are trained in the legal aspects of personal data protection and the risks involved in the processing of personal data;*
- *TNRS' Managing Board, through the IT Department, sets for each user the types of access and operations permitted to them and strictly necessary for the performance of their duties;*
- *The TNRS user/employee may process personal data only during the period in which he or she holds the said function.* TNRS provides for the extension or restriction of personal data processing assignments when a user/employee is in one of the following situations:

a) change of the work relationships;

b) modification of the duties related to processing of personal data, as set out in the job description.

The user's right of access to the personal data filing system is suspended during the period in which he or she is in one of the following situations:

a) unpaid leave, sick leave, parental leave or for a period longer than 3 months;

b) maternity leave or short-term disability leave;

c) follows a training or specialization with a program ending within more than 3 months;

d) during the course of a disciplinary investigation, where investigations regarding the processing of personal data in breach of the legal provisions are carried out with regard to the user;

e) other cases as provided by law.

- *When designing, maintaining, updating database management applications, access of the information system providers/programmers/maintenance personnel is prohibited to any personal data held/created/accessed by the TNRS staff in the said department. In such*

situations, only anonymous/pseudonymized data is made available to the providers/programmers/maintenance personnel;

- *In exceptional cases, only during the intervention and as limited by circumstances to the strictly necessary data, the persons providing technical support may have access to personal data only in the presence of a user designated by the operator, in this case, the responsibility for maintaining the confidentiality of the data belongs to such persons, who will therefore sign a Pledge of Confidentiality;*
- *The collection, introduction, modification and updating of personal data is carried out only by the personnel designated by the controller's managers in accordance with the internal rules;*
- *TNRS has the necessary technical measures to allow for the identification of the user who has introduced, modified or updated personal data;*
- *Owned/created personal databases and programs used by controllers/users are backed up with back-up solutions within a timeframe set by the TNRS management, depending on the size, volume and importance of such databases;*
- *TNRS designates/establishes users with service responsibilities and duties related to the backup of proprietary/created databases and of the programs used;*
- *Access to the premises where the documents containing personal data and/or access terminals/personal data processing equipment are located is limited to the users assigned by the controller's management and only for the performance of their service duties (restricted/controlled access);*
- *The documents, access terminals/equipment containing personal data are to be kept in cassettes and cabinets locked by key or other securing mechanisms and/or in lockable premises/areas. The documents that contain personal data used to carry out certain operations shall be handed over to the authorized persons or shall be locked immediately after the conclusion of such operations. The access terminals/equipment are to be secured with a password;*
- *The IT applications handling personal data shall automatically lock up the work session if the user fails to use the on-screen data for a set period of time, through work procedures/flow diagrams, depending on the operations to be performed.*
- *The access terminals must be set to the automatic screen saver function and the "lock screen - screen saver" function at a predetermined time delay through work procedures/flow diagrams, and if this is not technically feasible after expiry of the set time, the displayed data is to be hidden or the session closed. The access terminals used in relation to the public are positioned in such a way that the displayed data are only viewed by the users;*
- *The access of TNRS users/employees to personal data in the TNRS Network - servers and workstations, is controlled/restricted based on user names and passwords exclusively set by the IT Department, such users having limited access rights, according to the internal procedures (e.g., read only, write, execute, modify, full control, etc.);*

- *It is not allowed to remove from the organization mobile storage media (CD/DVD, USB Stick, Portable HDD, etc.) containing personal data, except based on the prior approval of TNRS management;*
- Using the e-mail service in any way that may lead to sending, distributing and delivering unsolicited e-mails in large volumes or unsolicited commercial messages ("Spam") shall be prohibited. By spam, we consider sending unsolicited commercial messages following which complaints are received from their recipients, using or distributing e-mail lists belonging to individuals who have not previously given their consent.
- *The users/employees shall not open SPAM/Malware messages and/or any other electronic communications that are unrelated to their employee activity. At the same time, TNRS employees are not allowed to host or to allow hosting websites or information the advertising of which is made by SPAM e-mails.* ***Failure to comply with the anti-spam policy shall be considered misconduct and shall be sanctioned in accordance with the Internal Rules.***
- *TNRS users/employees who process personal data are required to log out from their work session, lock the screen of the access terminals when they leave the workplace, and, at the end of the work schedule, turn off the access terminals;*
- *Only authorized users are allowed to print personal data and where the printing equipment allows it, this operation shall be controlled, based on a password.*

These rules and measures shall be complemented by the policies and procedures developed/implemented by the TNRS IT Department, such internal rules being necessary to ensure the adequate protection/safety of personal data.

8.1.4. Adherence to approved codes of conduct or approved certification mechanisms may be used as an element by which to demonstrate compliance with the obligations of the controller.

8.2. Data protection by design and by default

8.2.1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing (manual and/or automated means - e.g. operating systems, servers, workstations, security/backup/storage solutions, software solutions/IT applications purchased or developed in-house etc.) and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

8.2.2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such

measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

8.2.3. An approved certification mechanism as laid down in the specific legislation may be used as an element to demonstrate compliance with the requirements set out above.

8.3. Processor

8.3.1. Where processing is to be carried out on behalf of a controller, the controller shall contract only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

8.3.2. The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

8.3.3. *Processing by a processor shall be governed by a contract or other legal act under Union or domestic law, that is binding on the processor with regard to the controller* and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.

*That contract or other legal act shall stipulate, **in particular**, that the processor:*

a) *processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or domestic law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;*

b) *ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;*

c) *takes all appropriate technical and organizational measures to ensure an appropriate level of personal data security in accordance with the requirements of the specific legislation;*

d) *respects the mentioned conditions for engaging another processor;*

e) *taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights as laid down in the specific legislation;*

f) *assists the operator in ensuring compliance with obligations regarding the security of processing, the notification of a personal data breach to the Authority/data subject, data protection impact assessment, prior consultation, taking into account the nature of processing and the information available to the processor;*

g) *at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;*

h) *makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allows for and contributes to audits, including inspections, conducted by the controller or another auditor mandated by the controller.*

i) *The processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other data protection provisions in the Union or domestic law.*

8.3.4. Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to above shall be imposed on that other processor by way of a contract or other legal act under Union or domestic law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures.

Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.

8.3.5. Adherence to approved codes of conduct or approved certification mechanisms as laid down in the specific legislation may be used as an element by which to demonstrate sufficient guarantees as referred to above.

8.3.6. Without prejudice to an individual contract between the controller and the processor, the contract or the other legal act between the controller's processor and another processor may be based, in whole or in part, on standard contractual clauses provided for by/passed by the European Commission/supervisory authority, including when they are part of a certification granted to the controller or processor pursuant to specific legislation;

8.3.7. The contract or the other legal act referred to above shall be in writing, including in electronic form.

8.3.8. If a processor infringes this Regulation by determining the purposes and means of personal data processing, the processor shall be considered to be a controller in respect of that processing.

8.3.9. Where personal data are processed on behalf of TNRS by authorized processors (data processors - e.g. credit institutions, insurance companies, companies issuing printed or electronic vouchers, employee benefits cards, courier companies, etc.) TNRS' contractual partners shall conclude with each of these processors Personal Data Processing Agreements that will include the elements provided for in this Regulation and the specific legislation, previously established by the Data Protection Officer and approved by TNRS' management.

8.4. Processing under the authority of the controller or processor

The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or domestic law.

8.5. Records of processing activities

8.5.1. Organizations employing fewer than 250 persons shall not be obliged to maintain a record of personal data processing unless the processing they carry out is likely to result in a risk to the

rights and freedoms of the data subjects, the processing is not occasional or includes special categories of data or personal data relating to criminal convictions and offences, as provided for in the specific legislation.

8.5.2. If the controller is subject to the aforementioned provisions, it shall maintain a record of processing activities under its responsibility. That record shall contain the following information:

a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;

b) the purposes of the processing;

c) a description of the categories of data subjects and of the categories of personal data;

d) the categories of recipients to whom the personal data have been or will be disclosed, including recipients in third countries or international organisations;

e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and the documentation of suitable safeguards;

f) where possible, the envisaged time limits for erasure of the different categories of data;

g) where possible, a general description of the technical and organisational security measures;

8.5.3. Each controller and, where applicable, the controller's processor shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing:

a) the name and contact details of the processor or processors and of each controller on behalf of which that person (those persons) is(are) acting, and, where applicable, of the controller's or the processor's representative, as applicable;

b) the categories of processing carried out on behalf of each controller;

c) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and the documentation of suitable safeguards;

d) where possible, a general description of the technical and organisational security measures;

8.5.4. The records referred to above shall be in writing, including in electronic form.

8.5.5. The controller or the processor and/or the controller's or the processor's representative, shall make the record available to the supervisory authority on request, based on a prior notification submitted to the Controller;

8.6. Cooperation with the Supervisory Authority

TNRS, as the controller and the processor and, where applicable, their representatives, shall cooperate, on request, with the supervisory authority in the performance of its tasks.

8.7. Appropriate technical and organizational measures for personal data protection

8.7.1. General aspects regarding the security of processing

8.7.1.1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for

the rights and freedoms of natural persons, *the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia,* ***as appropriate****:*

a) the pseudonymisation and encryption of personal data;

b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

8.7.1.2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

8.7.1.3. Adherence to approved codes of conduct or approved certification mechanisms as laid down in the specific legislation may be used as an element by which to demonstrate compliance with the requirements referred to above.

8.7.1.4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or domestic law.

8.7.2. General aspects regarding the security of processing

At TNRS level, as a Personal Data Operator, the *IT technical and organizational measures provided for in the specific legislation, necessary for ensuring an appropriate level of protection are implemented* ***through:***

- **The identification, following specialized audit activities and the implementation/use in the performance of TNRS activity of appropriate IT technical solutions, taking into account the costs of implementation, the nature, scope, context, purposes of processing and related risks, solutions covering aspects provided for in the specific legislation, such as:**

✓ Basic security requirements: system security testing, system reinforcement, secure encryption, malware protection;

✓ Password policy: user authentication, two-factor authentication;

✓ Change management: separation of the testing environments, testing changes, developers' access;

✓ Access control: role-based access control, user account security, privileges review, Audit logs, unused accounts, technical users' privileges, security console, user information;

✓ Event management: log format log, log information, log protection and monitoring, log format, audited events;

✓ Data security: data encryption, data security through their lifecycle;

✓ Back-up: back-up copies, back-up software, back-up security, back-up verification, back-up viability;

✓ Personal data pseudonymization, minimization, integrity (computers, servers, access terminals, data printing), data availability, data erasure and portability, records of processing activities, etc.

- **Permanent development/implementation/monitoring by the IT Department of TNRS of certain personal data policies/specific protection procedures /security.**

8.7.3. Personal data mapping

For the purpose of mapping the personal data, the form (Annex 13) is to be filled in. The form is to be filled in or updated by the workplace supervisors with the support of other TNRS employees whenever changes occur regarding the nature of the activities carried out, the organizational structures, processed data, target categories, the introduction of new security measures, etc. The workplace supervisor is responsible for the accuracy and completeness of the information provided in this form and implicitly for ensuring the implementation of the security measures throughout the department, including following up the implementation of the department's/structure's Action Plans of Compliance with Regulation 2016/679 and training the subordinate staff on the application of the legislation on personal data protection. The completed form is kept in an electronic and physical format by each workplace supervisor.

If the implemented security measures are not appropriate, depending on the risks to data protection from the data subjects' perspective, the supervisor together with those responsible for implementing the measures proposes *Compliance Action Plans*. The data type, scope, context and purposes of the processing and use of new technologies shall be taken into account when assessing the risks.

8.7.4. GDPR rules for database management

Sending commercial communications for direct marketing purposes (e.g. Newsletters) to targeted natural persons identified in various TNRS records, databases, IT applications, by using email addresses such as lastname.firstname@gmail.com, lastname.firstname@yahoo.com or lastname.firstname@companyX.ro or other addresses containing personal data or personal telephone numbers (SMC) found in these records, in the absence of an informed consent previously given in an express, unambiguous and free manner by the data subjects, and clearly identified, shall be prohibited.

Commercial communications for direct marketing purposes may be made using email addresses such as lastname.firstname@gmail.com, lastname.firstname@yahoo.com or lastname.firstname@companyX.ro or other addresses containing personal data or personal telephone numbers (SMC) found in TNRS records, applications, databases, only to the extent that:

- we have obtained the express, unequivocal, previously given, informed consent of the data subjects, and

- the records, applications, databases used by TNRS shall be adapted so as to clearly distinguish the data subjects' consent for an effective control of this process in relation to GDPR, regardless of how it is obtained.

The data should be appropriate, relevant and strictly limited to what is strictly necessary for the purposes for which they are required for the underlying processing.

Each workplace manager, with the support of the IT Department, shall identify and take stock of, maintain in the organization's network, including in individual workstations, only those databases that are actually useful for performing the organization's current activity, as well as eliminate those which are no longer relevant to TNRS activity and/or whose retention period has expired. The list of databases managed by each office shall contain at least: the database name, storage location, person responsible for their management (development, modification), the persons with access rights, the retention period, the back-up frequency etc.

Each workplace supervisor who manages databases in the organization's network and on individual workstations, with the support of the IT Department, shall set up controlled/restricted access rules (e.g. Read only, write, execute, modify, etc.) for the users of such databases, revised as provided above, based on a user name and password, on access levels (if possible).

The databases should be grouped into dedicated folders, both those used for commercial activities/business relationships and the database used for direct marketing purposes targeted at natural persons.

In the organization's network, the workplace managers, with the support of the IT Department, shall only maintain documents containing personal data that are relevant, effectively useful for the performance of the TNRS current activity and remove all those that are not relevant, or are personal documents.

The IT Department shall permanently, in accordance with the approved programs, safeguard the personal databases as well as other documents containing personal data in the organization's network through back-up copies at agreed intervals.

8.8. Notification of a personal data breach to the supervisory authority

8.8.1. In the case of a personal data breach, TNRS through its Data Protection Officer shall notify the personal data breach to the supervisory authority competent without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the Authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

8.8.2. The processor shall notify the controller (notify the Data Protection Officer) without undue delay after becoming aware of a personal data breach.

8.8.3. The notification sent to the Authority regarding the personal data breach shall contain at least the following:

a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned;

b) the name and contact details of the data protection officer or other contact point where more information can be obtained;

c) describe the likely consequences of the personal data breach;

d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

8.8.4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

8.8.5. The controller, through the Data Protection Officer, shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with the specific legislation.

8.8.6. *TNRS employees are bound to immediately inform their direct supervisor and Data Protection Officer (e.g.: the following e-mail address is to be used administrator@sibfest.ro) in the event of a personal data breach.*

The Data Protection Officer shall analyse the information communicated and, if necessary, request further data and information from the functional entities.

If the personal data breach is reasonably justified, the Data Protection Officer shall draw up the Notification and request the opinion of the General Manager or Chief Secretary and the Chairperson's consent to send such a Notification to the Supervisory Authority.

The Notification shall be sent to the Supervisory Authority in paper or electronic form, as set out by the Authority.

8.9. Communication of a personal data breach to the data subject

8.9.1. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate, through the Personal Data Officer, the personal data breach to the data subject without undue delay.

8.9.2. The information provided to the data subject referred to above shall describe in clear and plain language the nature of the personal data breach and contain at least the following information and measures:

- the name and contact details of the data protection officer or other contact point where more information can be obtained;
- describe the likely consequences of the personal data breach;
- describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

8.9.3. The communication to the data subject shall not be required if any of the following conditions are met:

a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;

b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects concerned is no longer likely to materialise;

c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

CHAPTER 9 DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION

9.1. Data protection impact assessment

9.1.1. *Where a type of processing in particular using new technologies*, and taking into account the nature, scope, context and purposes of the processing, *is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, through the Data Protection Officer, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data*. A single assessment may address a set of similar processing operations that present similar high risks.

9.1.2. The Data Protection Officer develops, at the controller's request, in collaboration with TNRS employees, the impact assessment for a particular type of personal data processing.

9.1.3. *A data protection impact assessment shall in particular be required in the case of:*

a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

b) processing on a large scale of special categories of data or of personal data relating to criminal convictions and offences referred to in the specific legislation; or

c) a systematic monitoring of a publicly accessible area on a large scale.

9.1.4. *The supervisory authority shall establish and make public a list of the type of processing operations which are subject to the requirement for a data protection impact assessment.*

9.1.5. *The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required.*

9.1.6. *The assessment shall contain at least:*

a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;

b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

c) an assessment of the risks to the rights and freedoms of data subjects; and

d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

9.1.7. Compliance with approved codes of conduct referred to in the specific legislation by the relevant controllers or processors shall be taken into due account in assessing the impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment.

9.1.8. *Where appropriate, the controller, through the Data Protection Officer, shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.*

9.1.10. Where processing has a legal basis in Union law or in the law of the Member State to which the controller is subject, that law regulates the specific processing operation or set of operations in question, and a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis, the aforementioned provisions shall not apply unless Member States deem it to be necessary to carry out such an assessment prior to processing activities.

9.1.11. Where necessary, the controller, through the Data Protection Officer, shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.

9.2. Pre-consultation of the Supervisory Authority

9.2.1. *The controller, through the Data Protection Officer, shall consult the supervisory authority prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.*

9.2.2. When consulting the supervisory authority, the controller, through the Data Protection Officer, shall provide it with:

a) where applicable, the respective responsibilities of the controller, joint controllers and processors involved in the processing, in particular for processing within a group of undertakings;

b) the purposes and means of the intended processing;

c) the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to this regulation;

d) contact details of the personal data specialist;

e) data protection impact assessment; and

f) any other information requested by the supervisory authority.

9.2.3. Domestic law may require controllers to consult with, and obtain prior authorisation from, the supervisory authority in relation to processing by a controller for the performance of a task carried out by the controller in the public interest, including processing in relation to social protection and public health.

CHPATER 10 DATA PROTECTION OFFICER

10.1. Assignment of responsibilities/tasks to the Data Protection Officer

At TNRS, the tasks/responsibilities of the Data Protection Officer have been assigned to the Head of the Administrative Service - ***Data Protection Officer***.

The responsibilities assigned/established in the Job Description are as follows:

- Participates in the process of transition towards compliance with the General Data Protection Regulation (GDPR);
- notifies and advises TNRS or TNRS's processor as well as the employees of the organization dealing with the processing of personal data on the (national and European) obligations regarding the processing of personal data, as well as on any aspect related to personal data protection;
- advises and directly engages in data protection impact assessments, monitors their functioning, including pre-consultation of the supervisory authority, where applicable;
- monitors compliance with the (national and European) legal provisions and internal regulations on personal data protection at TNRS level;
- monitors the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
- participates in training the staff involved in personal data processing operations;
- participates in updating the records of personal data processing operations and monitors their correctness;
- monitors, using the sampling method, how natural persons whose personal data are being processed are informed of their rights;
- provides assistance with the management of personal data processing, maintenance of the personal data processing register as well as the security incidents register and issues notifications on personal data breaches;
- cooperates with the supervisory authority (ANSPDCP) and acts as a contact point in relation to the supervisory authority, the data subjects, as well as within TNRS in relation to processing issues;

10.2. TNRS Responsibilities in relation to the Data Protection Officer

- The management of TNRS and the heads of the functional entities within the organization shall ensure that the Data Protection Officer is appropriately and timely involved in all issues relating to personal data protection;
- The management of the TNRS and the heads of the functional entities within the organization shall support the Data Protection Officer by providing him or her with the resources necessary for the fulfilment of his or her tasks and access to personal data and processing operations, and which allow him or her to maintain his or her expert knowledge;
- The Data Protection Officer performs his or her activity within the TNRS. Within the performance of that activity, the Data Protection Officer shall not receive any instructions regarding the performance of his or her duties in relation to GDPR.
- The data subjects may contact and request expert assistance from the Data Protection Officer with regard to all issues related to data processing and the exercise of their rights;
- The management of TNRS and the Data Protection Officer shall ensure that any such tasks performed by this latter do not result in a conflict of interest.

CHAPTER 11 TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

11.1. Any decision to transfer data outside the EU and the European Economic Area shall be submitted for review to the Data Protection Officer prior to the transfer and in a timely manner.

Data transfers outside the EU and the European Economic Area may be performed:

- On the basis of an adequacy decision of the European Commission;
- Based on appropriate safeguards offered by TNRS or the TNRS's processor.

Appropriate safeguards may be provided for by:

a) a legally binding and enforceable instrument between public authorities or bodies;

b) binding corporate rules;

c) standard data protection clauses adopted by the European Commission;

d) standard data protection clauses adopted by a supervisory authority and approved by the European Commission;

e) an approved code of conduct together with binding and enforceable commitments of the TNRS or TNRS's processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or

f) an approved certification mechanism together with binding and enforceable commitments of the TNRS or TNRS's processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

11.2. Subject to the authorisation from the competent supervisory authority, *the appropriate safeguards may be provided for, in particular, by*:

a) contractual clauses between TNRS, TNRS's processor and the controller, the controller's processor or the recipient of the personal data in the third country or international organisation; or

b) provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.

11.3. *In the absence of an adequacy decision or appropriate safeguards,* ***a data transfer to a third country or an international organization shall take place only on one of the following conditions:***

a) the data subject concerned has explicitly consented to the proposed transfer after having been informed of the possible risks of such transfers for the data subject;

b) the transfer is necessary for the performance of a contract between the data subject and TNRS or the implementation of pre-contractual measures taken at the data subject's request;

c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between TNRS and another natural or legal person;

d) the transfer is necessary for important reasons of public interest;

e) the transfer is necessary for the establishment, exercise or defence of legal claims;

f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;

g) the transfer is made from a register which, according to Union or domestic law, is intended to provide information to the public and which is open to consultation by the public in general or by any person who can prove a legitimate interest.

11.4. *In the absence of a decision by the Commission, of appropriate safeguards and, in the absence of the aforementioned conditions,* ***a transfer to a third country or an international organization may take place only if:***

- the transfer is not repetitive;
- concerns only a limited number of data subjects;
- is necessary for the purposes of compelling legitimate interests pursued by the TNRS controller which are not overridden by the interests or rights and freedoms of the data subject and
- the controller has assessed all the circumstances regarding the data transfer and has, on the basis of that assessment, provided suitable safeguards with regard to the protection of personal data. The controller shall inform the supervisory authority of the transfer.

CHAPTER 12 SPECIFIC REMEDIES, LIABILITY AND PENALTIES

12.1. Right to lodge a complaint with a supervisory authority

12.1.1. Without prejudice to any other administrative or judicial remedy, every 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 this regulation.

12.1.2. The supervisory authority with which the complaint has been lodged shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy pursuant to specific legislation.

12.2. Right to an effective judicial remedy against a supervisory authority

12.2.1. Without prejudice to any other administrative or non-judicial remedy, each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.

12.2.2. Without prejudice to any other administrative or non-judicial remedy, each data subject shall have the right to an effective judicial remedy where the supervisory authority which is competent does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint lodged.

12.2.3. Proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established.

12.2.4. Where proceedings are brought against a decision of a supervisory authority which was preceded by an opinion or a decision of the European Data Protection Board in the consistency mechanism, the supervisory authority shall forward that opinion or decision to the court.

12.3. Right to an effective judicial remedy against a controller or controller's processor

12.3.1. Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under the law have been infringed as a result of the processing of his or her personal data in non-compliance with the legal provisions.

12.3.2. 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, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers.

12.4. Right to compensation and liability of the controller or processor

12.4.1. Any person who has suffered material or non-material damage as a result of an infringement of the specific legislation shall have the right to receive compensation from the controller or processor for the damage suffered.

12.4.2. Any controller involved in processing operations shall be liable for the damage caused by such processing operations which infringe the provisions of the specific legislation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of the specific legislation specifically directed to processors or where it has acted outside or contrary to lawful/contractual instructions of the controller.

12.4.3. A controller or processor shall be exempt from liability if it proves that it is not in any way responsible for the event giving rise to the damage.

12.5. General conditions for imposing administrative fines

12.5.1. The supervisory authority shall ensure that the imposition of administrative fines in respect of infringements of the provisions of the specific legislation shall in each individual case be effective, proportionate and dissuasive.

12.5.2. *Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in the specific legislation.*

The Authority may:

- issue warnings;

- issue reprimands;

- issue provisions;

- order the controller to communicate a personal data breach to the data subject;

- restrict or prohibit processing;

- order the rectification or erasure of data or restriction of processing.

If the controller is to be subject to administrative penalties for non-compliance with the personal data protection legislation, the Data Protection Officer shall consider lodging a claim against the administrative penalty and make proposals in relation with the possible remedy and, where appropriate, shall draft the complaint, and shall review at least the following:

a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected, and the level of damage suffered by them;

b) the intentional or negligent character of the infringement;

c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;

d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them;

e) any relevant previous infringements by the controller or processor;

f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

g) the categories of personal data affected by the infringement;

h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;

i) where measures referred to in the specific law have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;

j) adherence to codes of conduct or approved certification mechanisms; and

k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

The personal data officer will represent the controller in the administrative proceedings before the authority and in the event that the decision of the authority is contested before the courts.

12.5.3. Non-compliance with the GDPR provisions may be subject to administrative fines ranging from 10,000,000 EUR to 20,000,000 EUR or between 2% and 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

CHAPTER 13 RESPONSIBILITIES WITHIN TNRS

13.1. Appropriate knowledge and enforcement of this Regulation is a requirement for all TNRS personnel in accordance with the approved authority limits;

13.2. Responsibilities for personal data protection shall be gradually assigned to all TNRS personnel;

13.3. Responsibilities regarding the development, authorization, approval, implementation, monitoring and evaluation of the applicability of this Regulation, as well as the measures to be imposed, are as follows:

13.3.1. TNRS (with all organizational structures), as the Controller:

a) ensures the implementation of the Community-EU and domestic legislation on personal data protection at TNRS level though this Regulation or other internal acts;

b) ensures the compliance of all processing activities with the provisions of the Community-EU and domestic legislation on personal data protection;

c) ensures the provisions of information to data subjects and respects their rights;

d) takes the necessary steps to ensure personal data processing security;

e) ensures compliance with this regulation regarding the measures for the protection of individuals in relation to personal data processing.

13.3.2. The Board of Directors of TNRS approves this Regulation on the protection of personal data. **The Board of Directors of TNRS** shall oversee the implementation of the General Data Protection Regulation, including by ensuring that compliance issues are resolved effectively and promptly.

The Board of Directors of TNRS empowers the TNRS Manager to approve changes to this Regulation if legislative changes so require as a matter of urgency until further approved by **the Board of Directors of TNRS**.

13.3.3. TNRS Manager

a) Proposes the TNRS Regulation on the Personal Data Processing for approval to the **Board of Directors of TNRS**:

b) approves through internal regulatory/decision-making acts measures for the implementation of the relevant legal provisions and of the TNRS Regulation on personal data processing;

c) ensures by means of internal and external audit and/or control instruments to assess the processes related to this Regulation and the enforcement of the legislation in the area of data protection;

d) approves changes to this Regulation if legislative changes so require as a matter of urgency until further approved by **the Board of Directors of TNRS**.

13.3.4. The governing bodies of TNRS and the heads of its organizational structures (departments, services, offices, departments, etc.) are responsible for personal data protection for coordinated activities and, in this respect, have the following specific responsibilities:

a) determine the purposes and means of the processing of personal data when necessary within the context of performance of the commercial/contractual business and/or participation in festivals, local and international tours and/or specialized events organized by TNRS and/or in the premises under TNRS management, including the performance of the TNRS' current activity, and within the context of compliance with the legal obligations;

b) ensure the development/updating of their own procedures and, after their approval by the TNRS manager, implement them;

c) ensures the implementation and monitoring of compliance with the internal regulatory acts and specific legislation on personal data processing by the subordinate users (employees);

d) coordinate and monitor the activity of the staff as related to personal data protection as regards the controller;

e) ensure the users benefit from expert training in this area;

f) issue measures to complement or, where applicable, modify the users' job descriptions;

g) review and decide whether the users' right of access to personal data record systems under the law are to be suspended or revoked under the law;

h) establish organizational measures for the exercise of rights by the data subject;

i) coordinate the process of providing the necessary data and information to address the data subjects' requests;

j) keep track of the data subjects' requests in relation to the coordinated activities involving the processing of personal data;

k) periodically review the users' activity;

l) effectively inform the Data Protection Officer about the vulnerabilities and risks signalled in the personal data processing security system of the structure and proposes measures to rectify them;

m) effectively inform the Data Protection Officer about any breach of personal data protection rules that would prejudice the rights of the data subject, the measures taken to identify the person responsible and limit the effects of unauthorized dissemination of the data, as well as about whether recommendations have been issued or sanctions applied by the National Supervisory Authority or this latter has decided that prior checking or other investigations are to be performed.

13.3.5. **TNRS users and employees** respectively, who process personal data have the following specific responsibilities:

a) know and apply the provisions of the legal acts in the area of personal data processing as well as of this regulation;

b) inform the data subject when personal data are collected directly from him or her under the law as to: the identity of the controller, the purpose of the data processing, the recipients or categories of recipients of the data, the obligation to provide all the required data and the consequences of refusing to provide such data, the rights under law, the conditions under which such rights may be exercised, etc.;

c) process only the personal data necessary for the performance of their duties and assist their direct supervisors, the TNRS governing bodies, in order to perform their specific activities;

d) maintain the confidentiality of the processed data, user account, password/access code for the computer systems/databases through which personal data are managed;

e) comply with the security measures, as well as other rules established at TNRS level

f) immediately inform the direct supervisor and the Data Protection Officer (e.g.: the below e-mail address is to be used: administrator@sibfest.ro) about circumstances that may lead to unauthorized dissemination of personal data or a situation in which personal data have been accessed/processed in breach of the legal norms, of which he or she has become aware.

13.3.6. **TNRS Contract Managers**

a) have the responsibility/obligation to insert in the contracts they have concluded and are managing specific clauses (drafted by/together with the Data Protection Officer, more generally Annexes 5 and 6) regarding personal data protection and/or compliance with the General and Technical Conditions of Participation;

b) where personal data are processed on behalf of TNRS by authorized processors (data processors - e.g. credit institutions, insurance companies, companies issuing printed or electronic meal vouchers, employee benefits cards, courier companies, etc.) the Contract Managers shall

conclude with each of these processors Personal Data Processing Agreements that are to include the elements provided for in this Regulation and in the specific legislation, previously established by the Data Protection Officer and approved by TNRS' management.

c) if processing personal data for direct marketing purposes, the contract managers as well as the employees responsible for direct marketing operations (including IT-related services) shall necessarily take into account the consent given by the data subject prior to such processing in order to avoid situations of non-compliance with the legal provisions on personal data protection.

13.3.7. Data Protection Officer responsible for drafting the Regulation and process control, including: monitoring and controlling the unified application of the Regulation, compliance testing, specialized audits and the provision of information to the TNRS management; shall participate in the organization and management of continuous development programs for employees in the area of knowledge of the GDPR provisions; his or her responsibilities are provided for in this Regulation and in the Job Description.

13.3.8. Human Resources Specialist:

a) provides information to the TNRS employees and potential employees about the processing of personal data and their rights under the law;

b) participates in the organization and management of continuous development programs for employees in the area of personal data protection;

13.3.9. when hiring employees within TNRS, makes information available to them in order to inform them and raise their awareness about the provisions of this Regulation and ensures they sign the Compliance Commitment Annex 4,

13.3.10. IT Department - responsible for:

a) taking the technical and organizational measures, specific to the IT area, as provided for in this Regulation;

b) permanent development/implementation/monitoring of specific personal data protection/security policies/procedures at TNRS level.

c) training of users on specific personal data protection/security policies/procedures at **TNRS** level.

13.3.11. Administrative Service - responsible for providing technical support, respectively for displaying the Data Protection Information Sheets and applying the signs marking the existence of the video surveillance systems in those places where CCTV video surveillance cameras are installed. The security staff of the Administrative Service shall regularly check the physical state of the aforementioned information sheets and signage and shall be responsible for the security and confidentiality of the personal data stored in the video surveillance/monitoring system.

13.3.12. Management of companies performing outsourced activities or of the agents/intermediaries (where applicable) - process manager.

CHPATER 14 TNRS EMPLOYEES' COMPLIACE COMMITMENT TO THE SPECIFIC LEGISLATION AND TNRS PERSONAL DATA PROTECTION REGULATION

14.1. When hired, prior to the commencement of the personal data processing activities, but also subsequently, throughout their employment relationship, upon the organization of specific training sessions, all employees who process personal data shall sign an ***Individual Compliance Commitment*** to the specific legislation and this TNRS Personal Data Protection Regulation. *The Compliance Commitment form to be used is set out* ***in Annex 4;***

14.2. Written confirmation means the individual's commitment to comply with the specific legislation and the TNRS Personal Data Protection Regulation in order to protect TNRS's reputation.

14.3. The confirmation signature means that:

a) the employee has been informed about the provisions of the TNRS Personal Data Protection Regulation;

b) the employee has participated in the training programs and has been trained according to the provisions of the TNRS Regulation in this area;

c) the employee understands the importance of full compliance with the requirements of the specific legislation and the TNRS Personal Data Protection Regulation;

d) the employee assumes full responsibility in relation to compliance with the requirements laid down in the specific legislation and the TNRS Personal Data Protection Regulation;

e) the employee understands that, in the event of non-compliance with the principles and requirements included in the TNRS Personal Data Protection Regulation, he or she is directly responsible for breaching the individual commitment and the resulting consequences.

14.4. The refusal to sign the confirmation of the individual commitment means:

a) that it is necessary to identify the real reasons that have led to the refusal;

b) that additional training is required if the real reason is the incorrect understanding of the message or information sent;

c) that careful consideration of the employee concerned is necessary, followed by appropriate action, especially if he or she occupies a position that poses a sensitive risk to TNRS if the refusal to sign the confirmation is unfounded.

14.5. The Compliance Commitments signed by TNRS' employees shall be kept in the records of the Human Resources Specialist.

CHAPTER 15 TRAINING

15.1. The annual plans for continuous training, developed under the law, shall contain subjects related to knowledge of domestic and Community legislation on the processing of personal data as well as specific subjects regarding the risks presented by data processing and minimum-security measures, depending on the specificity of **TNRS** activity.

15.2. Periodically, the heads of the functional structures within the TNRS organize, with the support of the Data Protection Officer, training with users/employees to know the specific work procedures set up at TNRS level and on the risks posed by vulnerabilities and computer threats to processed personal data.

15.3. Training shall be regularly and mandatory attended upon the modification of the legal framework in this area, and incidents shall be processed together with all TNRS personnel involved in the personal data processing activity.

CHAPTER 16 FINAL PROVISIONS

16.1. Failure to comply with the provisions of this Regulation represents a major compliance risk that may result in penalties for TNRS from the competent regulatory/supervisory bodies under the law.

16.2. This Regulation is for "Internal Usage" only, its unauthorized dissemination by TNRS employees to third parties falls within the scope of the *Compliance Commitment* and shall be sanctioned in accordance with the legislation in force.

16.3. The application of administrative penalties shall not wipe out the criminal, civil, material or misdemeanour liability, where applicable, of the guilty persons.

16.4. This Regulation complements: the internal rules and procedures, flow diagrams, and any other internal regulatory acts.

16.5. If, following the date of entry into force of this Regulation, a legal provision amends/complements/repeals the provisions of this Regulation, the applicable legal provisions shall apply.

16.6. ***This Regulation shall enter into force on _____.***

General Manager of "RADU STANCA" NATIONAL THEATRE SIBIU

Constantin Chiriac

ANNEX 1

TO THE PERSONAL DATA PROTECTION REGULATION

INFORMATION NOTE ON PERSONAL DATA PROTECTION

Dear Applicant,

"Radu Stanca" National Theatre Sibiu, hereinafter referred to as TNRS, is a public cultural institution of interest for the municipality, with legal personality, funded from budget allocations granted by the Local Council of Sibiu Municipality and from extra-budgetary incomes under Law No. 273 2006 on local public finances, subordinated to the Local Council of Sibiu Municipality in accordance with Decision No.46/2001 of the Local Council of Sibiu Municipality. TNRS operates in accordance with the specific legislation as a repertory institution and as an institution that can bring together other artistic teams during a project to create artistic productions or co-productions to be performed only in determined series. TNRS is structured and operates according to the provisions of the Government Ordinance No. 21/2007 on institutions and companies specialised in the area of performance arts and concerts as well as in artistic agency activities, as approved with its subsequent amendments and additions by Law No. 353/2007, as amended by the Government Emergency Ordinance 48/2016, the provisions of this Regulation and the other legal provisions in force and is legally represented by Mr. Constantin Chiriac - General Manager.

TNRS processes the personal data of prospective employees (candidates) received directly from them or indirectly via specialised companies and/or recruitment/selection platforms (where applicable).

In order to fulfil the legal duties under the law and perform the current activity, including the performance of the contractual activity (as legitimate interests) and ensure the application of the legal provisions on the protection of natural persons with regard to personal data processing and the free movement of such data (domestic and Community law), TNRS shall safely manage and for the specified purpose only, the personal data provided.

TNRS shall not process personal data unless to the extent that this is necessary for the fulfilment of the aforementioned purpose, in compliance with the legal security and confidentiality provisions.

The purpose of the collection of personal data is to: recruit and select personnel, in this case your employment, in order to achieve the legitimate interest of TNRS (performing activities with the appropriate human resources). Subsequent processing of personal data for statistical purposes shall not be considered incompatible with the purpose of the collection if it is carried out in compliance with the applicable legal provisions.

Personal data means any information about an identified or identifiable natural person, namely: name and surname, gender, date and place of birth, citizenship, marital status, telephone/fax, home address/residence, e-mail, profession, workplace, professional training - diplomas-studies, family situation, image, interest, availability, etc. (basically all your CV).

In order to fulfil the aforementioned purpose, you are required to provide complete, up-to-date, accurate data, which is necessary for your recruitment/selection under the best conditions. ***Your refusal shall result in the impossibility to enter the employment contract if you are selected and accepted for the position you have applied for.***

The processing of personal data means any operation or set of operations that is performed on personal data whether by automated or non-automated means.

By signing this Note, you explicitly, unequivocally, freely and informally give your consent for TNRS to record and manage those data for the aforementioned purpose.

Recipients of personal data may be: the prospective employee-candidate or his or her legal representatives, TNRS' representatives, contract partners providing recruitment/selection services, judicial authorities, central and local public authorities, the Police, the Public Prosecutor's Office (within the limits of the legal provisions and/or as a result of expressly formulated requests), market research organizations (statistical purpose), etc.

TNRS uses personal information to better understand your needs and interests, to communicate with you, to carry out the recruitment/selection process for your prospective employment.

Your personal data confidentiality shall be ensured by TNRS and such data shall not be provided to third parties other than those provided for herein.

In order to fulfil the aforementioned purpose, TNRS shall process your personal data throughout the entire performance of the TNRS activities, until you or your legal representative exercise your right to object/erasure. Following the termination of the personal data processing operations for the purpose for which they had been collected, if you or your legal representative fails to exercise your right to object/erasure, the data shall be archived by TNRS for the period stipulated within TNRS internal procedures and/or shall be destroyed.

In order to prevent misuse of personal data as well as potential abuses, we use security methods and technologies along with appropriate work policies and procedures to protect the collected personal data.

According to the applicable legal provisions, you have the ***right of access, the right to rectification, the right to erasure of data, the right to restriction of processing, the right to data portability, the right to object and to automated individual decision-making. At the same time, you have the right to withdraw your consent at any time by sending a written notification to TNRS.***

In order to exercise those rights, you may contact the TNRS Data Protection Officer by sending a written request, dated and signed at the e-mail address: administrator@sibfest.ro or at the following mailing address: Bd. Corneliu Coposu nr. 2, Sibiu.

TNRS may, if necessary, request the data subject to provide additional information in order to establish his or her identity.

You are also granted the right to lodge a complaint with the competent supervisory authority and to seek a judicial remedy.

If any of your data is incorrect, please inform us as soon as possible.

Therefore, the undersigned:

_____

Date of birth: __ / __ / _____, Domicile: _____

Telephone: _____. E-mail: _____ ***expressly, unequivocally and freely agree with the processing of my personal data by TNRS headquartered in 2 Corneliu Coposu Blvd., Sibiu, e-mail: administrator@sibfest.ro for the purpose of recruitment/selection/employment, in accordance with the provisions of the legislation on the protection of natural persons in relation to the processing of personal data and the free movement of such data.***

I also declare that I have been informed about my rights as provided for in the specific legislation on the protection of natural persons in relation to the processing of personal data and the free movement of such data.

Date: Signature of the candidate:

Regards,

_____

ANNEX 2

TO THE PERSONAL DATA PROTECTION REGULATION

INFORMATION NOTE ON PERSONAL DATA PROTECTION

Dear Madam/Dear Sir acting as an employee of TNRS,

"Radu Stanca" National Theatre Sibiu, hereinafter referred to as TNRS, is a public cultural institution of interest for the municipality, with legal personality, funded from budget allocations granted by the Local Council of Sibiu Municipality and from extra-budgetary incomes under Law No. 273 2006 on local public finances, subordinated to the Local Council of Sibiu Municipality in accordance with Decision No.46/2001 of the Local Council of Sibiu Municipality. TNRS operates in accordance with the specific legislation as a repertory institution and as an institution that can bring together other artistic teams during a project to create artistic productions or co-productions to be performed only in determined series. TNRS is structured and operates according to the provisions of the Government Ordinance No. 21/2007 on institutions and companies specialised in the area of performance arts and concerts as well as in artistic agency activities, as approved with its subsequent amendments and additions by Law No. 353/2007, as amended by the Government Emergency Ordinance 48/2016, the provisions of this Regulation and the other legal provisions in force and is legally represented by Mr. Constantin Chiriac - General Manager.

TNRS processes the personal data of its own employees received directly or indirectly from them, including from publicly available sources, from public bodies/authorities/public institutions or institutions of public interest (entities with employment and social protection/security responsibilities, from the public records - criminal record) or the providers of services related to prevention or occupational medicine, working capacity evaluation, medical or social care etc.

In order to fulfil its duties set out by law and to perform its current activity (as legitimate interests) and ensure the application of the legal provisions on the protection of natural persons with regard to personal data processing and the free movement of such data (domestic law and Community law), TNRS shall safely manage and for the specified purpose only, the personal data provided.

TNRS shall not process personal data unless to the extent that this is necessary for the aforementioned purposes, in compliance with the legal security and confidentiality measures.

The purpose of the collection of personal data is: Effective management of the employment relationships arising from the IEC; Personnel management; Presence monitoring; Payroll, meal vouchers; Taxation; Occupational medicine appointments; Performance of TNRS commercial/contractual activity; Staff monitoring and supervision; Workplace misconduct investigations; Outstanding debts recovery; Vocational training; Archiving; Statistical purposes; Protection of objects, assets, values, persons and personal data; Prevention and combating of crimes; Internal communication; Communication with customers/suppliers; Communication with the public bodies/authorities/public institutions or institutions of public interest; Fulfilment of incumbent legal obligations; Performance of tasks established by law and of the current activity - legitimate interest.

The data subjects are the **TNRS** employees, their legal representatives/delegates and their family members.

"***Personal data***" means any information relating to an identified or identifiable natural person, namely: first name and last name, first name and last name of the family members, gender, date and place of birth, nationality, citizenship, signature, civil registration data, data extracted from the driving license/registration certificate, social security/health insurance number, telephone/fax, address (domicile/residence), e-mail, profession, workplace, professional training - diploma - studies, family status, military status, economic and financial status, salary, data regarding the property, banking data, habits/preferences/behaviour, image, voice, data processed through video surveillance systems and access/time cards, geolocation data/traffic data, IP address, cookie identifiers, Personal Numerical Code (CNP), passport ID and series, biometric

data, health data, criminal data, criminal convictions/security measures, on disciplinary/misdemeanour sanctions, criminal record data, etc.

In order to fulfil the aforementioned purpose, you are required to provide complete, up-to-date and accurate data. ***Your refusal shall result in the impossibility to enter into/perform the employment contract, fulfil the applicable legal obligations and the legitimate interests of TNRS and yourself.***

The processing of personal data means any operation or set of operations that is performed on personal data whether by automated or non-automated means.

Recipients of personal data may be: the employee or his/her legal representatives/delegates, TNRS representatives, clients, suppliers, banking companies, debt recovery companies, judicial authorities, central and local public authorities, the Police, Public Prosecutor's Office (within the limits of the legal provisions and/or as a result of expressly formulated requests), insurance and reinsurance companies, market research organizations (statistical purpose), etc.

Your personal data confidentiality shall be ensured by TNRS and shall not be provided to third parties other than those provided for herein.

In order to fulfil the aforementioned purpose, TNRS shall process your personal data throughout the entire performance of the TNRS activities, until you or your legal representatives exercise your right to object/erasure.

Following the termination of the personal data processing operations for the purpose for which they had been collected, if you or your legal representative fails to exercise your right to object/erasure, the data shall be archived by TNRS for the period stipulated within the TNRS internal procedures and/or shall be destroyed.

In order to prevent misuse of personal data as well as potential abuses, we use security methods and technologies along with appropriate work policies and procedures to protect the collected personal data.

Data transfers outside the EU and the European Economic Area may be performed:

only if:

the transfer is not repetitive;

concerns only a limited number of data subjects;

is necessary for the purposes of compelling legitimate interests pursued by the controller (TNRS) which are not overridden by the interests or rights and freedoms of the data subject and

According to the applicable legal provisions, you have the ***right of access, the right to rectification, the right to erasure of data, the right to restriction of processing, the right to data portability, the right to object and to automated individual decision-making. At the same time, you have the right to withdraw your consent at any time by sending a written notification to TNRS.***

In order to exercise those rights, you may contact the TNRS Data Protection Officer by sending a written request, dated and signed at the e-mail address: administrator@sibfest.ro or at the following mailing address: Bd. Corneliu Coposu nr. 2, Sibiu.

TNRS may, if necessary, request the data subject to provide additional information in order to establish his or her identity.

You are also granted the right to lodge a complaint with the competent supervisory authority and to seek a judicial remedy.

If any of your data is incorrect, please inform us as soon as possible.

Therefore, the undersigned:

_____

Date of birth: __ / __ / _____, Domicile: _____

Telephone: _____. E-mail: _____, hired for the Position/ Function_____/
Directorate_____

Office_____
_____

hereby declare that I have been informed about the processing of my personal data by TNRS, which is headquartered in Sibiu, Bd. Corneliu Coposu nr. 2, Sibiu, e-mail: administrator@sibfest.ro for the purpose mentioned herein, in accordance with the provisions of the legislation on the protection of natural persons in relation to the processing of personal data and the free movement of such data.

I also declare that I have been informed about my rights as provided for in the specific legislation on the protection of natural persons in relation to the processing of personal data and the free movement of such data.

Date: _____ Employee signature:

Regards,

_____

ANNEX 3

TO THE PERSONAL DATA PROTECTION REGULATION

INFORMATION REGARDING THE PROCESSING OF PERSONAL DATA BY VIDEO SURVEILLANCE SYSTEMS AT THE HEADQUARTERS OF TNRS

TNRS, through video surveillance systems, processes your personal data and your ***image. as well as other information permitting your identification.*** *- data belonging to employees, customers/prospective customers, visitors and any other person entering the TNRS headquarters in* ***Sibiu, Bd. Corneliu Coposu nr. 2.***

Images of identified or identifiable persons processed by video surveillance systems, constitute personal data:

a) even if they are not associated with the data subject's identification data or

b) even if they do not contain the image of the filmed person, but other information likely to lead to his or her identification (e.g. vehicle registration number).

In order to fulfil its duties set out by law and to perform its current activity (as legitimate interests) and ensure the application of the legal provisions on the protection of natural persons with regard to personal data processing and the free movement of such data (domestic law and Community law), TNRS shall safely manage and for the specified purpose only, the personal data provided. TNRS shall not process personal data unless to the extent that this is necessary for the fulfilment of the aforementioned purpose, in compliance with the legal security and confidentiality provisions.

The purpose of processing personal data is to: monitor/ensure the security of individuals, premises and/or private goods, prevent and combat crime, fulfil legal obligations and achieve legitimate interests.

The registered information is to be used by TNRS and may only be communicated to the following recipients: the data subject, the legal representatives/proxies of the data subject, the authorized representatives of TNRS, criminal prosecution/investigation bodies, law courts, according to the provisions of the domestic and community legislation applicable to the activity carried out by TNRS.

The storage period for the data obtained by video surveillance systems is 30 days, except where expressly regulated by law or in duly justified cases. Upon expiration of the term, the records shall be destroyed or deleted.

In order to prevent misuse of personal data as well as potential abuses, we use security methods and technologies along with appropriate work policies and procedures to protect the collected personal data.

Under the specific domestic and Community legislation on the protection of natural persons with regard to the processing of personal data and the free movement of such data, you have the ***right of access, the right to rectification, to erasure of data, the right to restriction of processing, the right to data portability, the right to object and to automated individual decision-making.***

In order to exercise those rights, you may contact the TNRS Data Protection Officer by sending a written request, dated and signed at the e-mail address: administrator@sibfest.ro or at the following mailing address: Bd. Corneliu Coposu nr. 2, Sibiu.

TNRS may, if necessary, request the data subject to provide additional information in order to establish his or her identity.

You are also granted the right to lodge a complaint with the competent supervisory authority and to seek a judicial remedy.

“Radu Stanca” National Theatre Sibiu

General Manager

Constantin Chiriac

ANNEX 4

TO THE PERSONAL DATA PROTECTION REGULATION

COMPLIANCE COMMITMENT

I hereby confirm that:

a) I have been informed about the provisions of the TNRS Personal Data Protection Regulation;

and/or

b) I have attended the training programs and I was trained according to the provisions of the TNRS Personal Data Protection Regulation (for the personnel attending professional training in this area after being hired).

I understand that I have the obligation to comply with the legal provisions on the processing of personal data, as well as the TNRS Personal Data Protection Regulation, considering my quality of employee of TNRS.

I personally assume responsibility for full compliance with the principles, requirements and obligations resulting from the legal provisions on the processing of personal data and the TNRS Personal Data Protection Regulation developed in application of the specific legal provisions.

I, the undersigned: **_____**

Date of birth: __ / __ / ____, hired for the Position/Function_____ / Department _____Office_____
___

Date: Signature:

The TNRS Personal Data Protection Regulation was presented by:

_____
__,

Function /Position _____ / Departamentul_____Office_____
____

Date: Signature:

Annex 5

TO THE PERSONAL DATA PROTECTION REGULATION

Personal data protection

"Radu Stanca" National Theatre Sibiu, hereinafter referred to as TNRS, is a public cultural institution of interest for the municipality, with legal personality, funded from budget allocations granted by the Local Council of Sibiu Municipality and from extra-budgetary incomes under Law No. 273 2006 on local public finances, subordinated to the Local Council of Sibiu Municipality in accordance with Decision No.46/2001 of the Local Council of Sibiu Municipality. TNRS operates in accordance with the specific legislation as a repertory institution and as an institution that can bring together other artistic teams during a project to create artistic productions or co-productions to be performed only in determined series. TNRS is structured and operates according to the provisions of the Government Ordinance No. 21/2007 on institutions and companies specialised in the area of performance arts and concerts as well as in artistic agency activities, as approved with its subsequent amendments and additions by Law No. 353/2007, as amended by the Government Emergency Ordinance 48/2016, the provisions of this Regulation and the other legal provisions in force and is legally represented by Mr. Constantin Chiriac - General Manager.

TNRS processes personal data under appropriate technical and organizational security conditions, the processing being carried out in compliance with the law in force.

TNRS processes personal data received directly from the data subjects within the performance of its duties as laid down by law, the performance of commercial/contractual relations and/or participation in festivals/tours/events organized by TNRS.

Personal data is being collected only based on your agreement/consent if deliberately and voluntarily offered, either on your own initiative or at the request of TNRS, for example through contract documents, the contract adhesion form, through one of the physical/online forms used, through the online contact form, online service purchase order form etc., newsletters subscription form, participation in events, raffles and contests, by filling in the account registration form on a TNRS website, etc.

Use of the TNRS websites is subject to the provisions herein and to the Terms and Conditions set out on these websites.

In order to fulfil its duties set out by law and in order to perform its current activity (as legitimate interests) and ensure the application of the legal provisions on the protection of natural persons with regard to personal data processing and the free movement of such data (domestic law and Community law), TNRS shall safely manage and for the specified purpose only, the personal data provided.

TNRS shall not process personal data unless to the extent that this is necessary for the fulfilment of the aforementioned purpose, in compliance with the legal security and confidentiality provisions.

Processing of personal data means any operation or set of operations that is performed on your personal data whether by automated or non-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, destruction, archiving;

Within the context of performance of its duties as laid down by law and the performance of TNRS current activity, including the performance of its commercial/contractual activity and/or the participation in tours, festivals and/or other specialized events organized by TNRS and/or within the premises of TNRS and within the context of fulfilment of its legal obligations, we may ask you to provide us with certain personal data, such as: name and surname, signature, telephone/fax, e-mail, workplace, position, PNC, ID/passport series and number etc.

The data subject(s) whose data may be processed by TNRS *exclusively for the purposes mentioned below are, where applicable:*

- TNRS natural persons customers, (current, former, existing or prospective), visitors, the general public, their legal or conventional representatives/delegates;

- Representatives/delegates/business contacts (business/contractual partners, exhibitors, co-exhibitors, organizers, co-organizers, suppliers, service providers, lessees etc. - current, former or prospective ones) and of the public institutions/authorities.

The data subjects are required to provide complete, up-to-date and accurate data. Refusal to provide such data may result in the impossibility to fulfil the contractual/business relationship and/or the impossibility to provide TNRS services.

By reading these provisions, and/or signing any document that provides personal data to TNRS, or by providing personal data in order to access the TNRS services and/or participate in events organized by TNRS and/or within the premises of TNRS, which is located in Sibiu, Bd. Corneliu Coposu nr.2, the data subjects are informed and/or expressly consent (agree) to the processing of personal data in accordance with the legal provisions on the protection of natural persons with regard to the processing of personal data and the free movement thereof (domestic law and Community-EU law).

Where data processing is no longer necessary for the provision of a service, the fulfilment of a legal obligation nor is it justified by a TNRS legitimate interest, the data subjects may refuse such processing or withdraw their previously given consent, such refusal producing its effects in the future. The data subjects may withdraw their consent to processing of their data for direct marketing purposes at any time and without the obligation to provide a reason. After the consent withdrawal request has been settled, the data subject will no longer receive commercial information regarding the events/fairs/services offered by TNRS.

The purpose of the collection of personal data is:

- Legal duties fulfilment by TNRS;
- Organization of shows, festivals, tours and other events/specialized events;
- Performance of TNRS commercial/contractual activity;
- Invoicing and collecting the value of the services provided by TNRS;
- Marketing, promotion, advertising, publicity, contests, advertising lotteries, including sending general or personalized commercial offers; service development and improvement;
- Operational management;
- Managing customer relationships; commercial communication with customers/suppliers by any means of communication;
- Fulfilment of incumbent legal obligations;
- Communicating with the public bodies/authorities/public institutions or institutions of public interest;
- Audit and control/supervision activities;
- Archiving, statistical purposes;
- Debt collection/Outstanding debts recovery;
- Settlement of disputes and litigations, enforcement of court decision, arbitration awards, court orders, etc.

TNRS shall treat all information collected from you as confidential and shall not share it with third parties (with the exception of organizers/co-organizers of events organized by TNRS and/or within the premises of TNRS, and/or of the business partners as this is the case described below) without your express and prior consent.

Recipients of the data may even be the data subject(s) who provided personal data as follows:

- TNRS natural person customers, (current, former, existing or prospective), visitors, the general public, their legal or conventional representatives/delegates (for the purpose of performing the commercial/contractual relationships);

- organizers, co-organizers, lessees, suppliers, service providers and other legal entities - TNRS business/contractual partners, public authorities/institutions;

The recipients (other than the data subjects) of the data may be:

- The central and local public authorities, judicial authorities, police, prosecutors (within the limits of the legal provisions and/or as a result of express requests), banking companies, bailiffs, insurance and reinsurance companies, market research organizations (statistical purpose) etc.

Personal data processing for promotional (marketing) purposes

The personal data provided by the data subjects (such as the name and surname, e-mail address, fax number, mobile/landline phone number) may be processed by TNRS only in compliance with their rights, in particular the right to information and objection, for the following purposes: marketing (including direct marketing), contests, advertising lotteries, commercial advertising for services provided by TNRS, including those developed together with a TNRS partner, by any means of communication, including electronic communication services. The personal data provided by the data subjects may be used for promotional (marketing) purposes and for the products or services of other TNRS partners, while observing the rights of the data subjects.

Should TNRS intend to use your data for direct marketing purposes (after the data subjects have opted accordingly), the data subjects shall be informed in advance. The data subjects may exercise their right to prevent such processing by ticking the appropriate boxes in the forms/documents used to collect personal data.

Whatever the case may be, if you would like your personal data not to be processed by *TNRS*, you may expressly request that any processing of data by TNRS be terminated. At the same time, when you no longer want to receive newsletters or information materials from *TNRS*, you can unsubscribe using the "*Dezabonare*" or "Unsubscribe" button.

Processing of personal data by video surveillance systems

TNRS, by video surveillance systems, processes personal data, such as image and other information permitting the identification of the data subjects.

Images of identified or identifiable persons processed by video surveillance systems, constitute personal data:

a) even if they are not associated with the data subject's identification data or

b) even if they do not contain the image of the filmed person, but other information likely to lead to his or her identification (e.g. vehicle registration number).

The purpose of processing personal data is to: monitor/ensure the security of individuals, premises and/or private goods, prevent and combat crime, fulfil legal obligations and achieve legitimate interests.

The registered information is to be used by TNRS and may only be communicated to the following recipients: the data subject, the legal representatives/proxies of the data subject, the authorized representatives of TNRS, criminal prosecution/investigation bodies, law courts, according to the provisions of the domestic and community legislation applicable to the activity carried out by TNRS.

The storage period for the data obtained by video surveillance systems is 30 days, except where expressly regulated by law or in duly justified cases. Upon expiration of the term, the records shall be destroyed or deleted.

In their relation with TNRS, the data subjects, according to the applicable legal provisions, have the following rights: the right of access, the right to rectification, the right to erasure of data, the right to restriction of processing, the right to data portability, the right to object and to automated individual decision-making.

Duration of personal data processing

In order to achieve the aforementioned purpose, TNRS shall process personal data throughout the performance of the *TNRS* activities until the data subject or legal representative exercises the right to object/erasure (unless TNRS processes data based on a legal obligation or justifying a legitimate interest). Following the termination of the personal data processing operations for the purpose for which they had been collected, if you or your legal representative fails to exercise your right to object/erasure, the data shall be archived by TNRS for the period stipulated within TNRS internal procedures and/or shall be destroyed.

In order to prevent misuse of personal data as well as potential abuses, we use security methods and technologies along with appropriate work policies and procedures to protect the collected personal data.

Full security of the data transmitted over the Internet can never be guaranteed. While TNRS is making every effort to protect personal data, the security of the data transmitted towards TNRS websites cannot be absolutely guaranteed. Any data transmission is at the risk of the data subjects. Once the personal data are received, TNRS uses strict security procedures and measures against the unauthorized and unlawful use, destruction, accidental loss or disclosure of personal data.

Data transfers outside the EU and the European Economic Area may *only* be performed under the conditions laid down by the specific domestic and EU legislation on the protection of natural persons with regard to the processing of personal data and the free movement thereof.

By reading and signing this contractual document, the Data Subjects confirm that they have been informed of their rights in accordance with the applicable legal provisions, namely: the right of access, the right to rectification, the right to erasure of data, the right to restriction of processing, the right to data portability, the right to object and to automated individual decision-making. At the same time, where processing is based on consent, the data subjects have the right to withdraw their consent at any time by means of a written notification sent to TNRS in accordance with the provisions of the applicable legislation, without affecting the lawfulness of processing based on consent before its withdrawal;

Also, the data subjects have the right to object at any time, free of charge and without any justification needed, to the processing of their personal data for direct marketing purposes, using, where appropriate, the unsubscribe function included in the marketing materials.

For the other purposes, the data subjects have the right to oppose at any time, free of charge, to the processing of the personal data they provide to TNRS, making reference to the intended data and purpose, only based on justified and legitimate reasons, in relation to their particular situation, unless TNRS provides evidence that it has legitimate and compelling reasons that justify such processing and which override the interests, rights and freedoms of the data subject or that the purpose is to establish, exercise or defend legal claims. In case of unjustified objection, TNRS shall be entitled to continue processing such data.

By reading this document, the data subjects have been informed about and understand that the personal data provided to TNRS are key elements for accessing the services provided by TNRS and/or the performance of the commercial/contractual activity.

If the data subjects, directly or through their representative, exercise the aforementioned rights in a manifestly unfounded, unjustified or excessive manner, in particular because of their repetitive character, TNRS may:

- charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested;
- or refuse to act on the request.

Also, if the data subjects, directly or through their representative, exercise the aforementioned right to object in a manifestly unfounded, unjustified or excessive manner, in particular because of their repetitive character, TNRS shall be entitled to consider the Contract concluded with the TNRS Customer as terminated without any other formality or court decision, except when subject to prior notice.

In order to exercise those rights, you may contact the TNRS Data Protection Officer by sending a written request, dated and signed at the e-mail address: administrator@sibfest.ro or at the following mailing address: Bd. Corneliu Coposu nr. 2, jud. Sibiu.

By signing this contractual document, you confirm that you have read, that you have been fully, correctly and accurately informed, that you have acknowledged and fully understand and agree with:

- the provisions herein;

- the provisions set out in the General and Technical Conditions of Participation of TNRS on the protection of personal data, which are an integral part of the contract;

- the fact that personal data shall be processed, as set out by the legislation in force, herein and in the General and Technical Conditions of Participation of TNRS (where applicable) both for the performance of this contract, the fulfilment of the legal obligations or legitimate interests of TNRS, and also based on your consent expressed through your option and by signing this document in a free, explicit unequivocal and informed manner, where processing such data for direct marketing purposes;

- TNRS shall process your personal data only to the extent that this is necessary for the purposes mentioned herein and within the General and Technical Conditions of Participation of TNRS (where applicable), in compliance with the legal provisions for data security and confidentiality.

The General and Technical Conditions of Participation of TNRS on the protection of personal data are fully available on the TNRS website.

Partner ***TNRS***

ANNEX 6

TO THE PERSONAL DATA PROTECTION REGULATION

PERSONAL DATA PROTECTION-CONTRACTS

TNRS processes personal data under appropriate technical and organizational security conditions, the processing being carried out in compliance with the law in force.

TNRS processes the personal data received directly from the data subjects within the performance of its duties as laid down by law, the performance of commercial/contractual relations and/or upon participation in the festivals/tours/events organized by TNRS and/or within the premises of the immovable property of TNRS, which is located on Bd. Corneliu Coposu nr. 2, Sibiu.

Personal data is collected only either based on your consent/agreement if it is deliberately and voluntarily offered, on your own initiative, or at the request of TNRS, for example by means of pre-contractual and/or contractual documents.

In order to perform the contract entered into with TNRS, to fulfil the duties set out by law, to perform the current activity (as legitimate interests) of TNRS and to ensure the application of the legal provisions on the protection of natural persons with regard to personal data processing (domestic law and Community law), TNRS shall safely manage and for the specified purpose only, the personal data provided.

TNRS shall not process personal data unless to the extent that this is necessary for the fulfilment of the aforementioned purpose, in compliance with the legal security and confidentiality provisions.

Processing of personal data means any operation or set of operations that is performed on your personal data whether by automated or non-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, destruction, archiving;

Within the context of performance of the duties laid down by law and the performance of the TNRS current activity, including the performance of the commercial/contractual activity and/or the participation in tours, festivals, shows and/or other specialized events organized by TNRS and/or within the premises of TNRS Bd. Corneliu Coposu nr.2, Sibiu, as well as in the context of the fulfilment of our legal obligations, we may request from your personal data, *such as:* name and surname, signature, telephone/fax, e-mail, workplace, position, PNC, ID/passport series and number etc.

The data subject(s) whose data may be processed by TNRS *exclusively for the purposes mentioned below are, where applicable:*

- TNRS natural persons customers, (current, former, existing or prospective), visitors, the general public, their legal or conventional representatives/delegates;

- Representatives/delegates/business contacts (business/contractual partners, exhibitors, co-exhibitors, festival participants, co-producers, organizers, co-organizers, suppliers, service providers, lessees etc. - current, former or prospective ones) and of the public institutions/authorities.

The data subjects are required to provide complete, up-to-date and accurate data. Refusal to provide such data may result in the impossibility to fulfil the contractual/business relationship and/or the impossibility to provide TNRS services.

By reading these provisions, and/or signing any document that provides personal data to TNRS, or by providing personal data in order to access the TNRS services and/or participate in the events organized by TNRS and/or within the premises of TNRS, which is located in Bd. Corneliu

Coposu nr.2, the data subjects are informed and/or expressly consent (agree) to the processing of personal data in accordance with the legal provisions on the protection of natural persons with regard to the processing of personal data and the free movement thereof (domestic law and Community-EU law).

The purpose of the collection of personal data is:

- Legal duties fulfilment by TNRS;
- Organization of shows, festivals, tours and other events/specialized events;
- Performance of TNRS commercial/contractual activity;
- Invoicing and collecting the value of the services provided by TNRS;
- Marketing, promotion, advertising, publicity, contests, advertising lotteries, including sending general or personalized commercial offers; service development and improvement;
- Operational management;
- Managing customer relationships; commercial communication with customers/suppliers by any means of communication;
- Fulfilment of incumbent legal obligations;
- Communicating with the public bodies/authorities/public institutions or institutions of public interest;
- Audit and control/supervision activities;
- Archiving, statistical purposes;
- Debt collection/Outstanding debts recovery;
- Settlement of disputes and litigations, enforcement of court decision, arbitration awards, court orders, etc.

TNRS shall treat all information collected from you as confidential and shall not share it with third parties (except for the organizers/co-organizers of the events organized by

TNRS and/or within the TNRS premises and/or those of its business partners, as described below) in the absence of your express and priorly given consent.

Recipients of the data may even be the data subject(s) who provided personal data as follows:

- TNRS natural person customers, (current, former, existing or prospective), visitors, the general public, their legal or conventional representatives/delegates (for the purpose of performing the commercial/contractual relationships);

- Festival participants, co-producers, organizers, co-organizers, lessees, suppliers, service providers and other legal entities - TNRS business/contractual partners, public authorities/institutions;

The recipients (other than the data subjects) of the data may be:

- The central and local public authorities, judicial authorities, police, prosecutors (within the limits of the legal provisions and/or as a result of express requests), banking companies, bailiffs, insurance and reinsurance companies, market research organizations (statistical purpose) etc.

Personal data processing for promotional (marketing) purposes

Personal data processing for promotional purposes (direct marketing) is an additional purpose of personal data processing as necessary for contract performance and does not condition the performance of the subject-matter of this contract (e.g.: provision of services). In this situation, the personal data shall be processed <u>only</u> based on your express, unambiguous, free, informed and previously given consent.

The personal data provided by you (such as the name and surname, e-mail address, fax number, mobile/landline phone number) may be processed by TNRS <u>only</u> based on your previously and freely given consent in an express, unambiguous and informed manner, in certain cases, in compliance with your rights, in particular the right to information and objection, for the following

purposes: direct marketing, contests, advertising lotteries, commercial advertising for the tasks fulfilled and services provided by TNRS, including those developed together with a TNRS partner, by any means of communication, including electronic communication services. The personal data provided by the data subjects may be used for promotional (marketing) purposes and for the products or services of other TNRS partners, while observing the rights of the data subjects.

The data subjects may exercise their right to prevent such processing by ticking the appropriate boxes in the forms/documents used to collect personal data.

Processing of personal data with a general identification function

Personal data with a general identification function (Personal Numerical Code - CNP, serial number and ID/passport number, etc.) shall be processed only where the identity of the data subjects must be established, and such processing is expressly provided for by a legal provision.

Processing of personal data by video surveillance systems in the case of data subjects at the TNRS headquarters.

TNRS, by video surveillance systems, processes personal data, such as image and other information permitting the identification of the data subjects.

The purpose of processing personal data is to: monitor/ensure the security of individuals, premises and/or private goods, prevent and combat crime, fulfil legal obligations and achieve legitimate interests.

The registered information is to be used by TNRS and may only be communicated to the following recipients: the data subject, the legal representatives/proxies of the data subject, the authorized representatives of TNRS, criminal prosecution/investigation bodies, law courts, according to the provisions of the domestic and community legislation applicable to the activity carried out by TNRS.

The storage period for the data obtained by video surveillance systems is 30 days, except where expressly regulated by law or in duly justified cases. Upon expiration of the term, the records shall be destroyed or deleted.

In their relation with TNRS, the data subjects, according to the applicable legal provisions, have the following rights: the right of access, the right to rectification, the right to erasure of data, the right to restriction of processing, the right to data portability, the right to object and to automated individual decision-making.

Duration of personal data processing

In order to achieve the aforementioned purpose, TNRS shall process personal data throughout the performance of TNRS activities until the data subject or legal representative exercises the right to object/erasure, withdraws his or her consent to personal data processing for direct marketing purposes (unless TNRS processes such data based on a legal obligation or justifying a legitimate interest). Following the termination of the personal data processing operations for the purpose for which they had been collected, if the data subject or his or her legal representative fails to exercise their right to object/erasure, under the law, and/or shall not withdraw his or her consent for direct marketing, those data shall be archived by TNRS for the period stipulated within TNRS internal procedures and/or shall be destroyed.

Data transfers outside the EU and the European Economic Area may <u>*only*</u> be performed under the conditions laid down by the specific domestic and EU legislation on the protection of natural persons with regard to the processing of personal data and the free movement thereof.

By reading and signing this contractual document, the Data Subjects confirm that they have been informed of their rights in accordance with the applicable legal provisions, namely: the right of access, the right to rectification, the right to erasure of data, the right to restriction of processing, the right to data portability, the right to object and to automated individual decision-making. Where processing is based on consent, the data subjects have the right to withdraw their consent at any time by means of a written notification sent to TNRS in accordance with the provisions of the applicable legislation, without affecting the lawfulness of processing based on consent before its withdrawal.

The data subjects have the right to object at any time, free of charge and without any justification needed, to the processing of their personal data for direct marketing purposes, using, where appropriate, the unsubscribe function included in the marketing materials.

For the other purposes, the data subjects have the right to oppose at any time, free of charge, to the processing of the personal data they provide to TNRS, making reference to the intended data and purpose, only based on justified and legitimate reasons, in relation to their particular situation, unless TNRS provides evidence that it has legitimate and compelling reasons that justify such processing and which override the interests, rights and freedoms of the data subject or that the purpose is to establish, exercise or defend legal claims. In case of unjustified objection, TNRS shall be entitled to continue processing such data.

By reading this document, the data subjects have acknowledged and understand that the personal data provided to TNRS are key elements for the fulfilment of the duties set out by law, the performance of the commercial/contractual activity and/or accessing the services provided by TNRS.

If the data subjects, directly or through their representative, exercise the aforementioned rights in a manifestly unfounded, unjustified or excessive manner, in particular because of their repetitive character, TNRS may:

- charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested;
- refuse to act on the request.

If the data subjects, directly or through their representative, exercise the aforementioned right to object in a manifestly unfounded, unjustified or excessive manner, in particular because of their repetitive character, TNRS shall be entitled to consider the Contract concluded with the TNRS Customer as terminated without any other formality or court decision, except when subject to prior notice.

In order to exercise those rights, you may contact the TNRS Data Protection Officer by sending a written request, dated and signed at the e-mail address: *administrator@sibfest.ro* or at the following mailing address: Bd. Corneliu Coposu nr. 2, Sibiu.

By signing this document, you confirm that you have read, that you have been fully, correctly and accurately informed, that you have acknowledged and fully understand and agree with:

- the provisions herein;

- the provisions set out in the General and Technical Conditions of Participation of TNRS on the protection of personal data (where the contract falls within the scope of such Conditions). The General and Technical Conditions of Participation of TNRS are available on the website www.tnrs.ro

- the fact that personal data shall be processed, as set out by the legislation in force, herein and in the General and Technical Conditions of Participation of TNRS (where the contract falls within the scope of such Conditions) in all cases, both for the performance of this contract, the fulfilment of the legal obligations or legitimate interests of TNRS, and also based on your consent expressed in a free, explicit, unequivocal and informed manner (where processing such data for direct marketing purposes);

- TNRS shall process your personal data only to the extent that this is necessary for the purposes mentioned herein and in the General and Technical Conditions of Participation of TNRS (where applicable), in compliance with the legal provisions for data security and confidentiality.

Also, by reading and signing this document, I declare that I have been informed about my rights under the specific legislation on the protection of personal data.

At the same time, based on the option below, I freely, explicitly and unequivocally give my informed consent to the processing of my personal data for direct marketing purposes:

YES ☐ NO ☐ Signature _____ Legal/Conventional Representative

YES □ NO □ Signature _____ Contact Person

TNRS **Partner**

_____ _____

_____
_____

Name and Function of other persons authorized by signature on behalf of contracting parties

Annex 7

TO THE PERSONAL DATA PROTECTION REGULATION

TNRS WEBSITE TERMS AND CONDITIONS
PERSONAL DATA PROTECTION

The Commitment of the "RADU STANCA" NATIONAL THEATRE SIBIU (TNRS) regarding the protection of personal data

Your trust in our services and staff is one of our main concerns. In this respect, in order to provide you with the best possible experience, we focus on continuous improvement throughout our entire activity.

TNRS is aware of the importance of your personal data and is committed to protecting their privacy and security. It is therefore important for us to provide you, in an integrated manner, with information regarding the processing of your personal under these Terms and Conditions.

"Radu Stanca" National Theatre Sibiu, hereinafter referred to as TNRS, is a public cultural institution of interest for the municipality, with legal personality, funded from budget allocations granted by the Local Council of Sibiu Municipality and from extra-budgetary incomes under Law No. 273 2006 on local public finances, subordinated to the Local Council of Sibiu Municipality in accordance with Decision No.46/2001 of the Local Council of Sibiu Municipality. TNRS operates in accordance with the specific legislation as a repertory institution and as an institution that can bring together other artistic teams during a project to create artistic productions or co-productions to be performed only in determined series. TNRS is structured and operates according to the provisions of the Government Ordinance No. 21/2007 on institutions and companies specialised in the area of performance arts and concerts as well as in artistic agency activities, as approved with its subsequent amendments and additions by Law No. 353/2007, as amended by the Government Emergency Ordinance 48/2016, the provisions of this Regulation and the other legal provisions in force and is legally represented by Mr. Constantin Chiriac - General Manager.

TNRS respects the confidentiality of all customers and the confidentiality of all visitors to our websites and shall treats/process your personal data with particular care, under appropriate technical and organizational security conditions.

TNRS processes the personal data received directly from you, as data subjects, or indirectly on the occasion of the performance of the commercial/contractual relationships and/or participation in fairs/events organized by TNRS and/or within the premises of TNRS.

Your personal data is collected only based on your consent/agreement, if deliberately and voluntarily offered, on your own initiative, for example through one of the online forms used, such as the online contact form, the online service purchase order form etc. by means of subscription to newsletters (of course, only after you have chosen to receive these newsletters), participation in raffles and contests, filling in the account registration form on a TNRS website, etc.

Using this website as well as other TNRS websites by you shall be subject to these provisions and to the General Terms and Conditions of TNRS.

If you do not agree with any of the terms of these terms and conditions, do not use any of our websites or do not provide us with your personal data. Some services may be subject to the provision of your personal data.

TNRS shall not process your personal data unless to the extent that this is necessary for the fulfilment of the aforementioned purpose, in compliance with the legal security and confidentiality provisions.

What kind of personal data does TNRS process?

Processing of personal data means any operation or set of operations that is performed on your personal data whether by automated or non-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, destruction, archiving.

To access TNRS websites, you do not need to provide us with any personal data.

In order to fulfil the legal duties under the law and perform the current activity, including the performance of the contractual activity and ensure the application of the legal provisions, including on natural persons with regard to personal data processing and the free movement of such data (domestic and Community-EU law), TNRS may request certain personal data.

To this end, TNRS may process, inter alia, the following personal data: Surname and name, telephone/fax, home/residence address, e-mail, profession, workplace, IP address, card no., card expiration date, CVV2/CVC2 code, etc.

Who are the data subjects?

The data subject(s) whose data may be processed by TNRS exclusively for the purposes mentioned below are:

- TNRS natural persons customers, (current, former, existing or prospective), visitors, the general public, their legal or conventional representatives/delegates;

- Representatives/delegates/business contacts (business/contractual partners, exhibitors, co-exhibitors, organizers, co-organizers, suppliers, service providers, lessees etc. - current, former or prospective ones) and of the public institutions/authorities.

Consequences of refusing the provision of personal data

As a data subject, you are required to provide complete, up-to-date and accurate data.

In order to provide you with specific services specific to TNRS, personal data shall be required as necessary for the provision of such services, and refusal to provide such data may result in the impossibility to provide the respective TNRS services.

When you purchase a service provided by TNRS, as well as when you participate in fairs/events/exhibition events organized by TNRS, we shall collect personal data in connection with the provision of such services. At the same time, as a visitor to the TNRS premises, we will collect personal data (image, video surveillance processed data etc.) in order to fulfil our legal obligations and conduct our current business (legitimate interest).

By reading these provisions, and/or signing any document through which personal data is provided to TNRS, or by providing personal data to access TNRS services or to participate in/purchase tickets/paying the fee for attending events organized by TNRS and/or on the premises of TNRS, the data subjects are informed and/or expressly give their consent (agreement) to the processing of personal data in accordance with the legal provisions on the protection of natural persons with regard to the processing of personal data and the free movement thereof (domestic law and Community-EU law).

Where data processing is no longer necessary for the provision of a service, the fulfilment of a legal obligation nor is it justified by a TNRS legitimate interest, the data subjects may refuse such processing or withdraw their previously given consent, such refusal producing its effects in the future. The data subjects may withdraw their consent for the processing of their data for direct marketing purposes at any time and without the obligation to provide a reason. After the consent withdrawal request has been settled, the data subject will no longer receive commercial information regarding the events/fairs/services offered by TNRS.

What are the purposes of the collection of personal data?

- Legal duties fulfilment by TNRS;

- Organization of festivals, shows, tours and other exhibition events/specialized events;

- Performance of TNRS commercial/contractual activity;

- Invoicing and collecting the value of the services provided by TNRS;

- Marketing, promotion, advertising, publicity, contests, advertising lotteries, including sending general or personalized commercial offers; service development and improvement;

- Operational management;

- Managing customer relationships; commercial communication with customers/suppliers by any means of communication;

- Fulfilment of incumbent legal obligations;

- Communicating with the public bodies/authorities/public institutions or institutions of public interest;

- Audit and control/supervision activities;

- Archiving, statistical purposes;

- Debt collection/Outstanding debts recovery;

- Settlement of disputes and litigations, enforcement of court decision, arbitration awards, court orders, etc.

TNRS shall treat all information collected from you as confidential and shall not share it with third parties (with the exception of organizers/co-organizers of events organized by TNRS and/or within the premises of TNRS, and/or of the business partners as this is the case described below) without your express and prior consent.

Who are the recipients of your personal data?

Recipients of the data may even be the data subject(s) who provided personal data as follows:

- TNRS natural person customers, (current, former, existing or prospective), visitors, the general public, their legal or conventional representatives/delegates (for the purpose of performing the commercial/contractual relationships);

- Festival participants, co-producers, organizers, co-organizers, lessees, suppliers, service providers and other legal entities - TNRS business/contractual partners, public authorities/institutions;

The recipients (other than the data subjects) of the data may be:

- The central and local public authorities, judicial authorities, police, prosecutors (within the limits of the legal provisions and/or as a result of express requests), banking companies, bailiffs, insurance and reinsurance companies, market research organizations (statistical purpose) etc.

Your personal data confidentiality shall be ensured by TNRS and such data shall not be provided to third parties other than those provided for herein.

Personal data processing for promotional (marketing) purposes

The personal data provided by the data subjects (such as the name and surname, e-mail address, fax number, mobile/landline phone number) may be processed by TNRS only in compliance with their rights, in particular the right to information and objection, for the following purposes: marketing (including direct marketing), contests, advertising lotteries, commercial advertising for services provided by TNRS, including those developed together with a TNRS partner, by any means of communication, including electronic communication services. The personal data provided by the data subjects may be used for promotional (marketing) purposes and for the products or services of other TNRS partners, while observing the rights of the data subjects.

Should TNRS intend to use your data for direct marketing purposes (after the data subjects have opted accordingly), the data subjects shall be informed in advance. The data subjects may exercise their right to prevent such processing by ticking the appropriate boxes in the forms/documents used to collect personal data.

Whatever the case may be, if you would like your personal data not to be processed by *TNRS*, you may expressly request that any processing of data by TNRS be terminated. At the same time, when you no longer want to receive newsletters or information materials from *TNRS*, you can unsubscribe using the "*Dezabonare*" or "Unsubscribe" button.

In your relationship with TNRS, you will be entitled to, in accordance with the applicable legal provisions, the following rights: *right of access, right to rectification, right to erasure of data, right to restriction of processing, the right to data portability, the right to object and to automated individual decision-making.*

Duration of personal data processing

In order to achieve the aforementioned purpose, TNRS shall process personal data throughout the performance of the TNRS activities until the data subject or legal representative exercises the right to object/erasure (unless TNRS processes data based on a legal obligation or justifying a legitimate interest). Following the termination of the personal data processing operations for the purpose for which they had been collected, if you or your legal representative fails to exercise your right to object/erasure, the data shall be archived by TNRS for the period stipulated within TNRS internal procedures and/or shall be destroyed.

What safety measures are used to protect your data?

In order to achieve the aforementioned purpose, TNRS shall process personal data throughout the performance of its duties, until the data subject or legal representative exercises the right to object/erasure (unless TNRS processes data based on a legal obligation or justifying a legitimate interest). Following the termination of the personal data processing operations for the purpose for which they had been collected, if you or your legal representative fails to exercise your right to object/erasure, the data shall be archived by TNRS for the period stipulated within TNRS internal procedures and/or shall be destroyed.

In order to prevent misuse of personal data as well as potential abuses, we use security methods and technologies along with appropriate work policies and procedures to protect the collected personal data.

Full security of the data transmitted over the Internet can never be guaranteed. While TNRS is making every effort to protect personal data, the security of the data transmitted towards TNRS websites cannot be absolutely guaranteed. Any data transmission is at the risk of the data subjects. Once the personal data are received, TNRS uses strict security procedures and measures against the unauthorized and unlawful use, destruction, accidental loss or disclosure of personal data.

Banking data security.

In the case of payments made by card (e.g.: online purchase of tickets), the sale shall be performed by means of online payment solutions offered by third parties authorized in their relationship with TNRS. In order to eliminate the risk that personal data may be abusively/illegally taken over and used by unauthorized persons, authorized third parties in their relationship with TNRS shall guarantee the legality and security of personal data (card number, expiration date, etc.) and of the computer systems used.

Conditions for data transfers outside the EU and European Economic Area

Data transfers outside the EU and the European Economic Area may <u>only</u> be performed under the conditions laid down by the specific domestic and EU legislation on the protection of natural persons with regard to the processing of personal data and the free movement thereof.

What are your rights?

By reading this document, the data subjects have been informed about the rights they are entitled to in accordance with the applicable legal provisions, namely: ***the right of access, the right to rectification, the right to erasure of data, the right to restriction of processing, the right to data portability, the right to object and to automated individual decision-making.*** At the same time, where processing is based on consent, the data subjects have the right to withdraw their consent at any time by means of a written notification sent to TNRS in accordance with the provisions of the applicable legislation, without affecting the lawfulness of processing based on consent before its withdrawal;

Also, the data subjects have the right to object at any time, free of charge and without any justification needed, to the processing of their personal data for direct marketing purposes, using, where appropriate, the unsubscribe function included in the marketing materials.

For the other purposes, the data subjects have the right to oppose at any time, free of charge, to the processing of the personal data they provide to TNRS, making reference to the intended data and purpose, only based on justified and legitimate reasons, in relation to their particular situation, unless TNRS provides evidence that it has legitimate and compelling reasons that justify such processing and which override the interests, rights and freedoms of the data subject or that the purpose is to establish, exercise or defend legal claims. In case of unjustified objection, TNRS shall be entitled to continue processing such data.

By reading this document, the data subjects have been informed about and understand that the personal data provided to TNRS are key elements for accessing the services provided by TNRS and/or the performance of the commercial/contractual activity.

If the data subjects, directly or through their representative, exercise the aforementioned rights in a manifestly unfounded, unjustified or excessive manner, in particular because of their repetitive character, TNRS may:

- charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested;

- or refuse to act on the request.

Also, if the data subjects, directly or through their representative, exercise the aforementioned right to object in a manifestly unfounded, unjustified or excessive manner, in particular because of their repetitive character, TNRS shall be entitled to consider the Contract concluded with the TNRS Customer as terminated without any other formality or court decision, except when subject to prior notice.

In order to exercise those rights, you may contact the TNRS Data Protection Officer by sending a written request, dated and signed at the e-mail address: *administrator@sibfest.ro* or at the following mailing address: Bd. Corneliu Coposu nr. 2, Sibiu.

A legible copy of the identity document of the signatory shall be attached to the request.

The data subjects are also granted the right to lodge a complaint with the competent supervisory authority and to seek a judicial remedy.

These provisions may be subject to occasional amendments/updates. We encourage you to check these provisions each time you use TNRS websites so that you are permanently informed about them. By accessing TNRS websites or using TNRS services via the mentioned websites, following the amendments, the new provisions shall be considered accepted.

Annex 8

TO THE PERSONAL DATA PROTECTION REGULATION

Subscribe to the Newsletter of "Radu Stanca" National Theatre in Sibiu (TNRS)

- Exclusive, promotional information
- Be the first to find out the news
- Tips and recommendations

☐ ***Place the check mark on the box***

I agree to receive information about the services, events and exhibition events organized by TNRS.

What does this mean? (link) The subscriber will be directed to the document "What does this mean?"

E-mail:

Subscribe

Note: You cannot subscribe without placing the check mark!!!!

TNRS values and respects the protection of your personal data. For further information, read TNRS Terms and Conditions (link)

What does this mean?

As a result of your consent, the representatives of "Radu Stanca" National Theatre in Sibiu (TNRS) may contact you to provide information (commercial communications) about the services, events, exhibition events organized by TNRS by e-mail, SMS and other digital channels, such as social networks.

In order to adapt the information you provided to your own behaviour and preferences and to offer you the best and most personalized experience, we may analyse and combine your personal data.

When we analyse and combine your personal data, we will only do so in accordance with the applicable legal provisions, which may involve obtaining prior approval or confirmation and/or additional information from you.

Such data may include:

The data that you want to actively share with us, such as your first and last name, e-mail address, home/residence address, telephone/fax number, profession, workplace, IP address, social networks, bank card no., etc.

TNRS allows you to withdraw your consent at any time.

For further information, please read TNRS Terms and Conditions (link)

Annex 9

TO THE PERSONAL DATA PROTECTION REGULATION

☐ ***Place the check mark on the box***

I have read and agree to the Terms and Conditions (link) of "Radu Stanca" National Theatre Sibiu (TNRS)

Note:

- ***if you do not place the check mark, we will not be able to set up your account for online payment of fees;***
- ***the check mark should also be applied by specialist visitors***

☐ ***Place the check mark on the box***

I agree to receive information about the services, events and exhibition events organized by TNRS and/or within the premises of TNRS and/or its business partners.

What does this mean? (link) The subscriber will be directed to the document "What does this mean?"

What does this mean?

As a result of your consent, the representatives of "Radu Stanca" National Theatre in Sibiu (TNRS) may contact you to provide information (commercial communications) about the services, events, exhibition events organized by TNRS by e-mail, SMS and other digital channels, such as social networks.

In order to adapt the information you provided to your own behaviour and preferences and to offer you the best and most personalized experience, we may analyse and combine your personal data.

When we analyse and combine your personal data, we will only do so in accordance with the applicable legal provisions, which may involve obtaining prior approval or confirmation and/or additional information from you.

Such data may include:

The data that you want to actively share with us, such as your first and last name, e-mail address, home/residence address, telephone/fax number, profession, workplace, IP address, social networks, bank card no., etc.

TNRS allows you to withdraw your consent at any time.

For further information, please read the TNRS Terms and Conditions (link)

Annex 10

TO THE PERSONAL DATA PROTECTION REGULATION

Request to exercise the right of access

To the attention of,

"Radu Stanca" National Theatre Sibiu, with the registered office in Corneliu Coposu nr. 2, Sibiu.

I, the undersigned _____ (*surname and first name*)

domiciled/residing in _____ street _____ no. _____ building ____ entrance ____ apartment __ telephone

_____, (*optional*) e-mail address _____ on the basis of Art. 15 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 *on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC* (General Data Protection Regulation), I hereby ask you to inform me whether my personal data are processed or not within your Organization.

Considering the above, please take the legal measures to ensure I receive the information requested under Regulation (EU) 2016/679 at the TNRS headquarters or at the following address _____, (*optional*) at the following electronic mailing address

_____.

DATE: SIGNATURE:

Annex 11

TO THE PERSONAL DATA PROTECTION REGULATION

Request to exercise the right of access

To the attention of,
"Radu Stanca" National Theatre Sibiu, Bd. Corneliu Coposu nr. 2, Sibiu.

I, the undersigned _____ (*surname and first name*)

domiciled/residing in _____ street _____ no. _____ building ____ entrance ____ apartment ___ telephone

_____, (*optional*) e-mail address _____ on the basis

of Art. 16 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 *on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC* (General Data Protection Regulation), I hereby ask you to take the legal measures so that the following categories of personal data related to me _____[1] may be rectified as they are incomplete/inaccurate.

At the same time, please notify the third parties _____ [2] to whom the following personal data concerning me have been disclosed _____ [3] that those data have been rectified.

(where applicable) Evidence of the need for rectification is based on _____

(Or) Please find attached the following original/copy documents on which this request is based: _____
_____

DATE: SIGNATURE:

[1], [3] The concerned personal data shall be listed.
[2] Specify who they are, to the extent that their identity is known.

Annex 12

TO THE PERSONAL DATA PROTECTION REGULATION

Request for exercising the right of erasure of data

To the attention of,
"Radu Stanca" National Theatre Sibiu, Bd. Corneliu Coposu nr. 2, Sibiu.

I, the undersigned _____ (*surname and first name*)

domiciled/residing in _____ street _____ no. _____ building ____ entrance ____ apartment __ telephone

_____, (*optional*) e-mail address_____
based on Art. 17 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 *on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC* (General Data Protection Regulation), I hereby ask you to take the legal measures so that the personal data concerning me _____[4] may be erased.

as they have been _____
[5]

At the same time, please notify the third parties _____ [6] to whom the following personal data concerning me have been disclosed _____ [7] that those data have been erased.

(Or) Please find attached the following original/copy documents on which this request is based: _____
_____

_____
_____

In view of the above, please ensure that the information about the actions taken according to my request are communicated to me at the TNRS headquarters or at the following address _____, (*optional*) at the following e-mail address
_____
_____.

DATE: SIGNATURE:

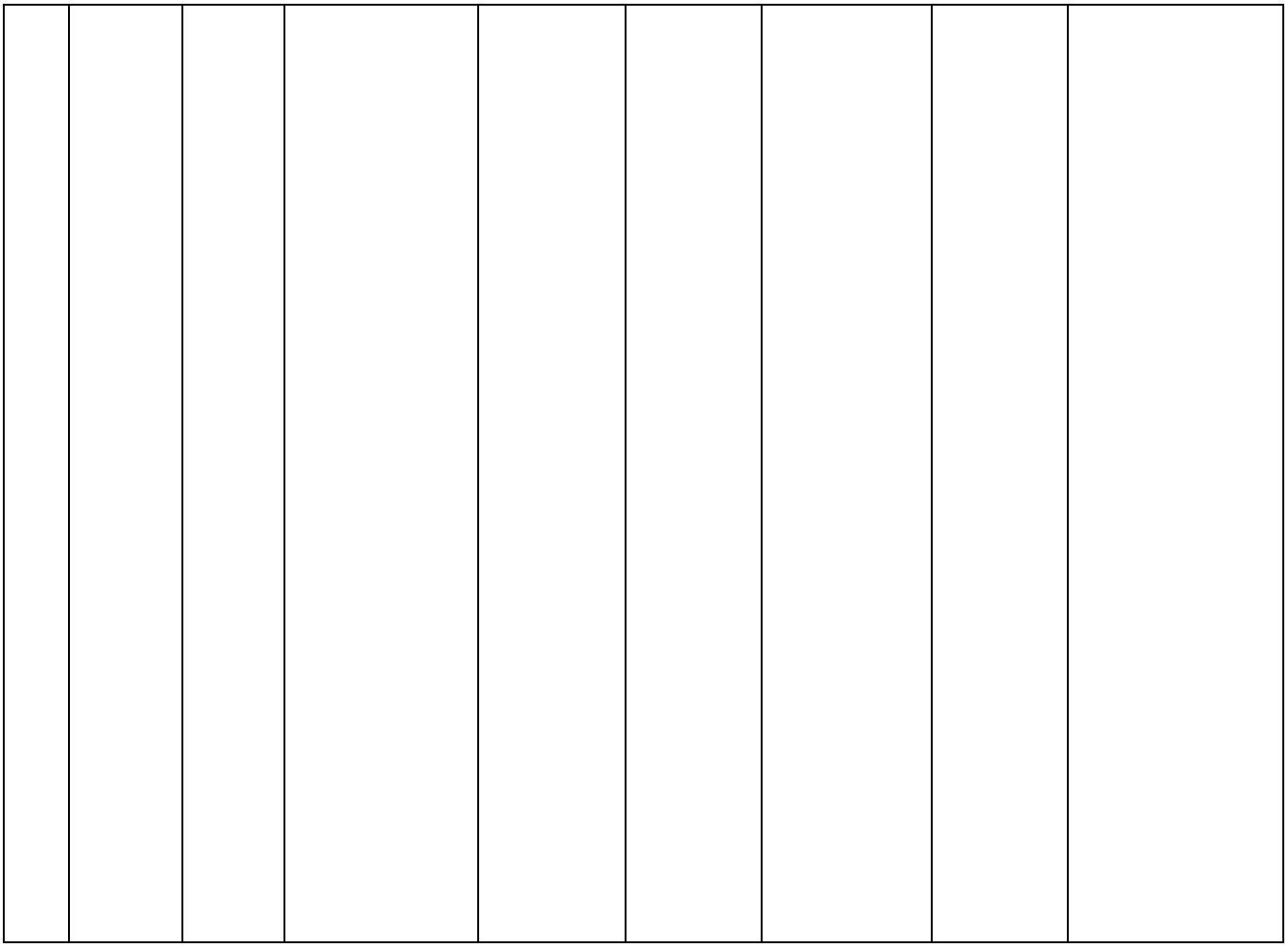
Annex 13

[4] , [3] The concerned personal data shall be listed.
[5] Please fill in with the reason;
[4] Specify who they are, to the extent that their identity is known.

TO THE PERSONAL DATA PROTECTION REGULATION

Data processed by TNRS

Entity	What	Who	Why	Where	Until	Is communicated to	From	How/security measures
Natural persons	a) surname first name; b) CNP (Personal Numerical Code); c) domicile; d) identity document series/no.; e) contact details (phone number, e-mail address); f) studies; g) job history, h) image i) bank account j) criminal record k) medical data; l) about relatives and affiliates m) financial data	a) employees / prospective employees; b) former employees; c) participants / Project applicants; d) Visitors /event participants; f) Representatives members/companies; g) Clients/ trainees /subscribers; h) experts nominated within the offers for calls for proposals; i) reviewers; j) trainees; k) members.	a) Fulfilment of legal obligations/duties: - statement/taxation; - drafting/issuance; documents regarding the status of employee - performance of occupational medicine control; - professional development courses; - payments related to the employee/insured status; - verification of eligibility for projects benefiting from external funding; - organization of the "National Top of Private Companies in Romania"; - organization of national and international fairs in Romania and Romania's participation in fairs and exhibitions abroad under the national pavilion; b) Fulfilment of contractual obligations, c) Press accreditations d) Marketing: - Sending newsletters; - sending invitations to events;	a) TNRS headquarters - within the structure that uses the data; - within the TNRS archive b) On the server hosting the TNRS website, in a database - external server.	a) According to the archive list b) By the time of unsubscription (the data shall not be erased)	a) The data are communicated to third parties for the performance of a legal duty/requirement and/or the exercise of a right. b) The data are communicated to third parties for the fulfilment of a contractual obligation: - occupational medicine; - payments regarding the employee/insured status; - professional training; - event attendance.	The data are collected: a) from public registers; b) from the data subject; c) communicated by third parties for the fulfilment of a legal/contractual obligation; d) from external public sources - websites.	a) The data are archived; - in physical form, on paper - **access to people with tasks and unregulated access!** - in electronic form, internal and external storage media, **unregulated access!** b) The data are processed manually/automatically.



Legal entities: customers	a) Company name b) Address, contact details (tel., fax, e-mail, website); c) Tax Identification Number, registration number; d) representatives (name, date of birth, place of birth, CNP); e) Shareholders (natural persons: name, date of birth, place of birth/legal person: name, Unique Identification Code) f) financial data; g) data on exported goods;	clients Companies incorporated in Romania	a) Fulfilment of legal duties: - organization and preparation of shows, tours - organization of the "Sibiu Performing Arts Market". - organization of the "International Theatre Festival in Sibiu"; b) fulfilment of contractual obligations c) Marketing - Sending newsletters; - Sending invitations to events; d) editing publications	TNRS headquarters - within the structure that uses the data; - within the TNRS archive.	a) According to the archive list b) by the termination of the contractual relationship; b) by the time of unsubscription.	a) The data are communicated to third parties for the performance of a legal duty/requirement and/or the exercise of a right. b) The data are communicated to third parties for the fulfilment of a contractual obligation:	The data are collected: a) from public registers; b) from the data subject; c) communicated by third parties for the fulfilment of a legal/contractual obligation; d) from external public sources - websites.	

Annex 14

TO THE PERSONAL DATA PROTECTION REGULATION

GENERAL AND TECHNICAL CONDITIONS OF PARTICIPATION

General conditions:

I. PERSONAL DATA PROTECTION

This section sets out the conditions for the processing of personal data applicable to all customers (exhibitors, co-exhibitors, organizers, co-organizers, lessees, suppliers, etc.), their partners, visitors, their representatives and the general public visiting, regardless of their status, the TNRS building located in Bd. Corneliu Coposu nr.2, Sibiu and/or participating in the events organized by TNRS.

"Radu Stanca" National Theatre Sibiu (TNRS) is aware of the importance of your personal data and is committed to protecting their privacy and security. It is therefore important for us to provide you, in an integrated manner, with information regarding the processing of your personal data within these General conditions.

TNRS processes personal data under appropriate technical and organizational security conditions, the processing being carried out in compliance with the law in force.

TNRS processes the personal data received directly from the data subjects (including via TNRS websites or, indirectly on the occasion of the performance of the commercial/contractual relationships and/or participation, regardless of their status, in the events organized by TNRS and/or within the premises of TNRS.

Personal data is being collected only based on your agreement/consent if deliberately and voluntarily offered, either on your own initiative or at the request of TNRS, for example through contract documents, the contract adhesion form, through one of the physical/online forms used, through the online contact form, online service purchase order form etc., newsletters subscription form, participation in raffles and contests, by filling in the account registration form on a TNRS website or using the application etc.

Use of the TNRS websites is subject to the provisions herein and to the Terms and Conditions set out on these websites.

If you do not agree with any of the terms of these provisions on personal data protection, do not use any of TNRS websites or do not provide us with your personal data. Some services may be subject to the provision of your personal data.

In order to fulfil the legal duties under the law and perform the current activity, including the performance of the contractual activity and ensure the application of the legal provisions on the protection of natural persons with regard to personal data processing and the free movement of such data (domestic and Community law), TNRS shall safely manage and for the specified purpose only, the personal data provided.

TNRS shall not process personal data unless to the extent that this is necessary for the aforementioned purposes, in compliance with the legal security and confidentiality measures.

Processing of personal data means any operation or set of operations that is performed on personal data whether by automated or non-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, destruction, archiving;

To access TNRS websites, you do not need to provide any kind of personal data.

Within the context of performance of TNRS current activity, including the performance of the commercial/contractual activity and/or the participation in tours, festivals and/or other specialized events organized by TNRS and/or within the premises of TNRS, involving the acquisition of TNRS services offered on websites, online payment of fees of newsletters subscription, and within the context of fulfilment of its legal obligations, TNRS may ask you to provide us certain personal data.

To this end, TNRS may process, inter alia, the following personal data: surname and first name, signature, data extracted from the driving license/registration certificate (in certain cases), telephone/fax, domicile/residence address, e-mail, profession, workplace, banking data, habits/preferences/behaviour, image, voice, data processed by video surveillance systems, IP address, credit card data (card no., card expiry date, CVV2/CVC2 code), IBAN code, Personal Numerical Code (CNP), identity document/passport ID and serial number.

The data subject(s) whose data may be processed by TNRS exclusively for the purposes mentioned below are:

- TNRS natural person customers, (current, former, existing or prospective), spectators, the general public, their legal or conventional representatives/delegates;

- - Representatives/delegates/business contacts (business/contractual partners, cultural partners, co-producers, organizers, co-organizers, suppliers, service providers, lessees etc. - current, former or prospective ones) and of the public institutions/authorities.

The data subjects are required to provide complete, up-to-date and accurate data.

In order to provide you with specific services specific to TNRS, personal data shall be required as necessary for the provision of such services, and refusal to provide such data may result in the impossibility to provide the respective TNRS services.

When you purchase a service provided by TNRS, as well as when you participate in events/exhibition events organized by TNRS, we shall collect personal data in connection with the provision of such services. At the same time, as a visitor to the TNRS premises, we will collect personal data (image, video surveillance processed data etc.) in order to fulfil our legal obligations and conduct our current business (legitimate interest).

By reading these provisions, and/or signing any document through which personal data is provided to TNRS, or by providing personal data to access TNRS services or to participate in/purchase tickets/paying the fee for attending events organized by TNRS and/or on the premises of TNRS, the data subjects are informed and/or expressly give their consent (agreement) to the processing of personal data in accordance with the legal provisions on the protection of natural persons with regard to the processing of personal data and the free movement thereof (domestic law and Community-EU law).

Where data processing is no longer necessary for the provision of a service, the fulfilment of a legal obligation nor is it justified by a TNRS legitimate interest, the data subjects may refuse such processing or withdraw their previously given consent, such refusal producing its effects in the future. The data subjects may withdraw their consent for the processing of their data for direct marketing purposes at any time and without the obligation to provide a reason. After the consent withdrawal request has been settled, the data subject will no longer receive commercial information regarding the events/fairs/services offered by TNRS.

The purpose of the collection of personal data is:

- Legal duties fulfilment by TNRS;
- Organization of festivals, tours, performing arts market and other exhibition events/specialized events;
- Performance of TNRS commercial/contractual activity;
- Invoicing and collecting the value of the services provided by TNRS;
- Marketing, promotion, advertising, publicity, contests, advertising lotteries, including sending general or personalized commercial offers; service development and improvement;
- Operational management;
- Managing customer relationships; commercial communication with customers/suppliers by any means of communication;
- Fulfilment of incumbent legal obligations;
- Communicating with the public bodies/authorities/public institutions or institutions of public interest;
- Audit and control/supervision activities;
- Archiving, statistical purposes;
- Debt collection/Outstanding debts recovery;
- Settlement of disputes and litigations, enforcement of court decision, arbitration awards, court orders, etc.

TNRS shall treat all information collected from you as confidential and shall not share it with third parties (with the exception of organizers/co-organizers of events organized by TNRS and/or within the premises of TNRS, and/or of the business partners as this is the case described below) without your express and prior consent.

Recipients of the data may even be the data subject(s) who provided personal data as follows:

- TNRS natural person customers, (current, former, existing or prospective), visitors, the general public, their legal or conventional representatives/delegates (for the purpose of performing the commercial/contractual relationships);

- Festival participants, participants in the performing arts market, organizers, co-organizers, lessees, suppliers, service providers and other legal entities - TNRS business/contractual partners, public authorities/institutions;

The recipients (other than the data subjects) of the data may be:

- The central and local public authorities, judicial authorities, police, prosecutors (within the limits of the legal provisions and/or as a result of express requests), banking

companies, bailiffs, insurance and reinsurance companies, market research organizations (statistical purpose) etc.

Personal data processing for promotional (marketing) purposes

The personal data provided by the data subjects (such as the name and surname, e-mail address, fax number, mobile/landline phone number) may be processed by TNRS only in compliance with their rights, in particular the right to information and objection, for the following purposes: marketing (including direct marketing), contests, advertising lotteries, commercial advertising for services provided by TNRS, including those developed together with a TNRS partner, by any means of communication, including electronic communication services. The personal data provided by the data subjects may be used for promotional (marketing) purposes and for the products or services of other TNRS partners, while observing the rights of the data subjects.

Should TNRS intend to use your data for direct marketing purposes (after the data subjects have opted accordingly), the data subjects shall be informed in advance. The data subjects may exercise their right to prevent such processing by ticking the appropriate boxes in the forms/documents used to collect personal data.

Whatever the case may be, if you would like your personal data not to be processed by *TNRS*, you may expressly request that any processing of data by TNRS be terminated. At the same time, when you no longer want to receive newsletters or information materials from TNRS, you can unsubscribe using the "*Dezabonare*" or "Unsubscribe" button.

Processing of personal data with a general identification function

Personal data with a general identification function (Personal Numerical Code - CNP, serial number and ID/passport number, etc.) shall be processed only where the identity of the data subjects must be established, and such processing is expressly provided for by a legal provision.

Processing of personal data by video surveillance systems

TNRS, by video surveillance systems, processes personal data, such as image and other information permitting the identification of the data subjects.

Images of identified or identifiable persons processed by video surveillance systems, constitute personal data:

a) even if they are not associated with the data subject's identification data or

b) even if they do not contain the image of the filmed person, but other information likely to lead to his or her identification (e.g. vehicle registration number).

The purpose of processing personal data is to: monitor/ensure the security of individuals, premises and/or private goods, prevent and combat crime, fulfil legal obligations and achieve legitimate interests.

The registered information is to be used by TNRS and may only be communicated to the following recipients: the data subject, the legal representatives/proxies of the data subject, the authorized representatives of TNRS, criminal prosecution/investigation bodies, law courts, according to the provisions of the domestic and community legislation applicable to the activity carried out by TNRS.

The storage period for the data obtained by video surveillance systems is 30 days, except where expressly regulated by law or in duly justified cases. Upon expiration of the term, the records shall be destroyed or deleted.

In their relationship with TNRS, the data subjects shall be entitled, in accordance with the applicable legal provisions, to the following rights: *the*

right of access, the right to rectification, the right to erasure of data, the right to restriction of processing, the right to data portability, the right to object and to automated individual decision-making.

Duration of personal data processing

In order to achieve the aforementioned purpose, TNRS shall process personal data throughout the performance of the TNRS activities until the data subject or legal representative exercises the right to object/erasure (unless TNRS processes data based on a legal obligation or justifying a legitimate interest). Following the termination of the personal data processing operations for the purpose for which they had been collected, if you or your legal representative fails to exercise your right to object/erasure, the data shall be archived by TNRS for the period stipulated within TNRS internal procedures and/or shall be destroyed.

In order to prevent misuse of personal data as well as potential abuses, we use security methods and technologies along with appropriate work policies and procedures to protect the collected personal data.

Full security of the data transmitted over the Internet can never be guaranteed. While TNRS is making every effort to protect personal data, the security of the data transmitted towards TNRS websites cannot be absolutely guaranteed. Any data transmission is at the risk of the data subjects. Once the personal data are received, TNRS uses strict security procedures and measures against the unauthorized and unlawful use, destruction, accidental loss or disclosure of personal data.

No information security software is infallible.

In the case of payments made by card (e.g.: online service purchase/fee payment), the sale shall be performed by means of online payment solutions offered by third parties authorized in their relationship with TNRS. In order to eliminate the risk that personal data may be abusively/illegally taken over and used by unauthorized persons, authorized third parties in their relationship with TNRS shall guarantee the legality and security of personal data (card number, expiration date, etc.) and of the computer systems used.

Data transfers outside the EU and the European Economic Area may **only** be performed under the conditions laid down by the specific domestic and EU legislation on the protection of natural persons with regard to the processing of personal data and the free movement thereof.

By reading this document, the data subjects have been informed about the rights they are entitled to in accordance with the applicable legal provisions, namely: ***the right of access, the right to rectification, the right to erasure of data, the right to restriction of processing, the right to data portability, the right to object and to automated individual decision-making.*** At the same time, where processing is based on consent, the data subjects have the right to withdraw their consent at any time by means of a written notification sent to TNRS in accordance with the provisions of the applicable legislation, without affecting the lawfulness of processing based on consent before its withdrawal;

Also, the data subjects have the right to object at any time, free of charge and without any justification needed, to the processing of their personal data for direct marketing purposes, using, where appropriate, the unsubscribe function included in the marketing materials.

For the other purposes, the data subjects have the right to oppose at any time, free of charge, to the processing of the personal data they provide to TNRS, making reference to the intended data and purpose, only based on justified and legitimate reasons, in relation to their particular situation, unless TNRS provides evidence that it has legitimate and compelling reasons that justify such processing and which override the interests, rights

and freedoms of the data subject or that the purpose is to establish, exercise or defend legal claims. In case of unjustified objection, TNRS shall be entitled to continue processing such data.

By reading this document, the data subjects have acknowledged and understand that the personal data provided to TNRS are key elements for accessing the services provided by TNRS and/or the performance of the legal duties/requirements and /or commercial/contractual activity.

If the data subjects, directly or through their representative, exercise the aforementioned rights in a manifestly unfounded, unjustified or excessive manner, in particular because of their repetitive character, TNRS may:

- charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested;
- refuse to act on the request.

Also, if the data subjects, directly or through their representative, exercise the aforementioned right to object in a manifestly unfounded, unjustified or excessive manner, in particular because of their repetitive character, TNRS shall be entitled to consider the Contract concluded with the TNRS Customer as terminated without any other formality or court decision, except when subject to prior notice.

In order to exercise those rights, the data subjects may contact the TNRS Data Protection Officer by sending a written request, dated and signed at the e-mail address: *administrator@sibfest.ro* or at the following mailing address: TNRS, Bd. Corneliu Coposu nr. 2, Sibiu. A legible copy of the identity document of the signatory shall be attached to the request.

The data subjects are also granted the right to lodge a complaint with the competent supervisory authority and to seek a judicial remedy.

Annex 15

TO THE PERSONAL DATA PROTECTION REGULATION

Surname/Name:	
Mailing address:	
Phone/Fax:	
E-mail:	
Social Media Account:	
Profession/Function:	
Workplace:	

INFORMATION/CONSENT STATEMENT FOR DIRECT MARKETING PURPOSES WITHIN THE CONTEXT OF PERSONAL DATA PROCESSING

Dear Applicant,

Not long ago you decided to become the partner of "Radu Stanca" National Theatre Sibiu (TNRS), including by accessing our services.

We hereby want to thank you for the benefits of our collaboration with you.

As part of our relationship development strategies, TNRS wants to continue/develop our professional collaboration with you, respectively with the company/institution that you represent.

A part of the responsibility that rests with TNRS in our relationship with you is also the manner in which we take care of your personal data that you have made available to us earlier, throughout the performance of our commercial/contractual relationships, which we expect to continue in our future professional collaboration as well.

Your trust in our services and staff is one of our main concerns. In this respect, in order to provide you with the best possible experience, we focus on continuous improvement throughout our entire activity.
TNRS is aware of the importance of your personal data and is committed to protecting their privacy and security.
It is therefore important for us to provide you, in an integrated manner, the information regarding the processing of your personal data, within this document.
Detailed information is available on the website: www.tnrs.ro (ex: General and Technical Conditions of Participation of TNRS, Terms and Conditions).
We therefore inform you that, as of 25 May 2018, Regulation 2016/679/EU on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR) shall be applied by all Member States of the European Union. This Regulation seeks

to create a unified and uniform legislative framework across the European Union so that national implementation measures may no longer be required.

Considering that TNRS is bound to align to the GDPR provisions and taking into account that we want to maintain and develop the professional collaboration with you, we believe this is the right time to highlight a few important aspects.

"Radu Stanca" National Theatre Sibiu, hereinafter referred to as TNRS, is a public cultural institution of interest for the municipality, with legal personality, funded from budget allocations granted by the Local Council of Sibiu Municipality and from extra-budgetary incomes under Law No. 273 2006 on local public finances, subordinated to the Local Council of Sibiu Municipality in accordance with Decision No.46/2001 of the Local Council of Sibiu Municipality. TNRS operates in accordance with the specific legislation as a repertory institution and as an institution that can bring together other artistic teams during a project to create artistic productions or co-productions to be performed only in determined series. TNRS is structured and operates according to the provisions of the Government Ordinance No. 21/2007 on institutions and companies specialised in the area of performance arts and concerts as well as in artistic agency activities, as approved with its subsequent amendments and additions by Law No. 353/2007, as amended by the Government Emergency Ordinance 48/2016, the provisions of this Regulation and the other legal provisions in force and is legally represented by Mr. Constantin Chiriac - General Manager.

TNRS respects the confidentiality of all customers and shall treat/process your personal data with particular care, under appropriate technical and organizational security conditions.

TNRS processes the personal data received directly from you, as data subjects, or indirectly within the performance of duties as laid down by law, the performance of commercial/contractual relations and/or upon participation in the shows/tours/events organized by TNRS and/or within the premises of the immovable property of TNRS, which is located in Sibiu, Bd. Corneliu Coposu nr. 2.

Personal data is collected only either based on your consent/agreement if deliberately and voluntarily offered, on your own initiative, or at the request of TNRS, for example via pre-contractual, contractual documents, filling in of forms such as declarations, online forms etc.)

TNRS shall not process your personal data unless to the extent that this is necessary for the fulfilment of the aforementioned purpose, in compliance with the legal security and confidentiality provisions.

What kind of personal data does TNRS process?

Processing of personal data means any operation or set of operations that is performed on your personal data whether by automated or non-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, destruction, archiving;

Within the context of performance of the duties laid down by law and the performance of TNRS current activity, including the performance of the commercial/contractual activity and/or the participation in shows, festivals, and/or other specialized events organized by TNRS and/or within the premises of TNRS, which is located in Sibiu, Bd. Corneliu Coposu nr.2, as well as within the context of fulfilment of legal obligations, we may request certain personal data.

To this end, TNRS may process, inter alia, the following personal data: Surname and name, mailing address, telephone/fax, e-mail, social media account, profession, workplace,

Who are the data subjects?

The data subject(s) whose data may be processed by TNRS exclusively for the purposes mentioned below are:

- TNRS natural persons customers, (current, former, existing or prospective), visitors, the general public, their legal or conventional representatives/delegates;

- Representatives/delegates/business contact natural persons (business/contractual partners, co-producers, organizers, co-organizers, suppliers, service providers, lessees etc. - current, former or prospective ones) and of the public institutions/authorities.

By reading these provisions, by providing personal data for the purpose of promoting services, events and exhibitions organized by/at TNRS and the maintenance/development of our commercial/contractual relationships, you are informed and expressly consent to (agree with) the processing of personal data in accordance with the legal provisions on the protection of natural persons with regard to the processing of personal data and the free movement thereof (domestic law and Community-EU law).

What are the purposes of the collection of personal data?

We use your personal data for the following **purposes**:

- Legal duties fulfilment by TNRS;
- Organization of shows, festivals, tours and other events/specialized events;
- Performance of TNRS commercial/contractual activity;
- Invoicing and collecting the value of the services provided by TNRS;
- Marketing, promotion, advertising, publicity, contests, advertising lotteries, including sending general or personalized commercial offers; service development and service improvement;

- Operational management;
- Managing customer relationships; commercial communication with customers/suppliers by any means of communication;

- Fulfilment of incumbent legal obligations;
- Communicating with the public bodies/authorities/public institutions or institutions of public interest;
- Audit and control/supervision activities;
- Archiving, statistical purposes;
- Debt collection/Outstanding debts recovery;
- Settlement of disputes and litigations, enforcement of court decision, arbitration awards, court orders, etc.
-

TNRS shall treat all information collected from you as confidential and shall not share it with third parties (except for the organizers/co-organizers of certain events organized by TNRS and/or within the premises of the immovable property of TNRS located in Sibiu, Bd. Corneliu Coposu nr.2, Sibiu, and/or its business partners, as described below) in the absence of your express and priorly given consent.

Who are the recipients of your personal data?

Recipients of the data may even be the data subject(s) who provided personal data as follows:

- - TNRS natural person customers, (current, former, existing or prospective), visitors, the general public, their legal or conventional representatives/delegates (for the purpose of performing the commercial/contractual relationships);
- Representatives/delegates/business contacts (business/contractual partners, exhibitors, co-exhibitors, organizers, co-organizers, suppliers, service providers, lessees etc. - current, former or prospective ones) and of the public institutions/authorities.

The recipients (other than the data subjects) of the data may be:

- Central and local public authorities, judicial authorities, police, prosecutors (within the limits of the legal provisions and/or as a result of express requests) etc.

Your personal data confidentiality shall be ensured by TNRS and such data shall not be provided to third parties other than those provided for herein.

Personal data processing for promotional (marketing) purposes

The personal data provided by the data subjects (such as the name and surname, e-mail address, fax number, mobile/landline phone number etc.) may be processed by TNRS only based on your previously and freely given consent in an express, unambiguous and informed manner, in compliance with your rights, in particular the right to information and objection, for the following purposes: marketing (including direct marketing), contests, advertising lotteries, commercial advertising for services provided by TNRS, including those developed together with a TNRS partner, by any means of communication, including by electronic communication services. The personal data provided by you may be used for TNRS promotional purposes and for the products or services of other TNRS partners, while in compliance with your rights.

You may exercise your right to prevent such processing by ticking the appropriate boxes in the forms/documents used to collect personal data.

Whatever the case may be, if you would like your personal data not to be processed by TNRS, you may expressly request that any processing of your data by us be terminated. At the same time, when you no longer want to receive newsletters or information materials from TNRS, you can unsubscribe using the "*Dezabonare*" or "Unsubscribe" button.

In your relation with TNRS, you will be entitled to, in accordance with the applicable legal provisions, the following rights: *the right of access, the right to rectification, the right to erasure of data, the right to restriction of processing, the right to data portability, the right to object and to automated individual decision-making.*

Duration of personal data processing

In order to achieve the aforementioned purpose, TNRS shall process your personal data throughout the performance of the TNRS activities until you or your legal/conventional representative exercises the right to object/erasure (unless TNRS processes data based on a legal obligation or justifying a legitimate interest). Following the termination of the personal data processing operations for the purpose for which they had been collected, if you or your legal representative fails to exercise your right to object/erasure, the data shall be archived by TNRS for the period stipulated within TNRS internal procedures and/or shall be destroyed.

What safety measures are used to protect your data?

In order to prevent misuse of personal data as well as potential abuses, we use security methods and technologies along with appropriate work policies and procedures to protect the collected personal data.

Full security of the data transmitted over the Internet can never be guaranteed. Once we receive your personal data, we shall use strict security procedures and measures against the unauthorized and unlawful use, destruction, accidental loss or disclosure of personal data.

Conditions for data transfers outside the EU and European Economic Area

Data transfers outside the EU and the European Economic Area may **only** be performed under the conditions laid down by the specific domestic and EU legislation on the protection of natural persons with regard to the processing of personal data and the free movement thereof.

What are your rights?

By reading this document, you have been informed about the rights you are entitled to, in accordance with the applicable legal provisions, namely: ***the right of access, the right to rectification, the right to erasure of data, the right to restriction of processing, the right to data portability, the right to object and to automated individual decision-making.***

You have the right to object at any time, free of charge and without any justification, to the processing of your personal data for direct marketing purposes, using, where appropriate, the unsubscribe function included in the marketing materials.

By reading and filling in this document, you have acknowledged and understand that the personal data provided to TNRS represents key elements for receiving information regarding the services, events and exhibitions organized by/within TNRS and/or the performance of the commercial/contractual activity.
If, directly or through your representative, you exercise the aforementioned rights in a manifestly unfounded, unjustified or excessive manner, in particular because of the repetitive character, TNRS may:

- either charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested;
- refuse to act on the request.

You are also granted the right to lodge a complaint with the competent supervisory authority and to seek a judicial remedy.

How can you exercise your rights?

In order to exercise those rights, you may contact the TNRS Data Protection Officer by sending a written request, dated and signed at the e-mail address: administrator@sibfest.ro or at the following mailing address: Bd. Corneliu Coposu nr. 2, Sibiu.

By signing and filling in this contractual document, you confirm that you have read, that you have been fully, correctly and accurately informed, that you have acknowledged and fully understand and agree with:

- the provisions herein;

- the provisions set out in the General and Technical Conditions of Participation of TNRS on the protection of personal data. The General and Technical Conditions of Participation of TNRS are available on the website TNRS.ro where applicable);

- personal data processing, as set out by the legislation in force, herein and in the General and Technical Conditions of Participation of TNRS (where applicable) shall be processed both for direct marketing purposes (promotion of services, events and manifestations organized by TNRS and/or within the premises of TNRS in Sibiu, Bd. Corneliu Coposu nr. 2, and for the maintenance/development of the commercial/contractual relations based on your informed consent freely, explicitly and unequivocally given;

- TNRS shall process your personal data only to the extent that this is necessary for the purposes mentioned herein and in the General and Technical Conditions of Participation of TNRS (where applicable), in compliance with the legal provisions for data security and confidentiality.

I understand that I may revoke this approval statement at any time, free of charge and without any justification, and in such case the revocation shall be applied in accordance with the applicable legal provisions.

Also, by reading and filling in this document, I declare that I have been informed about my rights under the specific legislation on the protection of personal data.

At the same time, based on the option below, I freely, explicitly and unequivocally give my informed consent to the processing of my personal data for direct marketing purposes:

YES ☐ *NO* ☐

I agree with the provision of information/documents relating to the services, events and exhibitions of TNRS and/or performed within the premises of TNRS, which is located in Sibiu, Bd. Corneliu Coposu nr,2, (which TNRS considers might be of benefit to me), by:

- telephone calls at the specified telephone number: 0269.210,092.

- by mail, at the specified postal address: Bd. Corneliu Coposu nr. 2, Sibiu.

- electronic mail, at the specified e-mail address: administrator@sibfest.ro

Annex 16

TO THE PERSONAL DATA PROTECTION REGULATION
Processor - Contracts

Processing by a processor shall be governed by a contract or other legal act under Union or domestic law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.

Where processing is to be carried out on behalf of TNRS, only processors providing sufficient guarantees for the implementation of the appropriate technical and organisational measures in such a manner that processing may meet the requirements of this Regulation and ensure the protection of the rights of the data subject shall be contracted.

Clauses and safeguards

1. The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

2. The processor:

j) *processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or domestic law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;*

k) *ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;*

l) *takes all appropriate technical and organizational measures to ensure an appropriate level of personal data security in accordance with the requirements of the specific legislation;*

m) *respects the mentioned conditions for engaging another processor;*

n) *taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights as laid down in the specific legislation;*

o) *assists the operator in ensuring compliance with obligations regarding the security of processing, the notification of a personal data breach to the Authority/data subject, data protection impact assessment, prior consultation, taking into account the nature of processing and the information available to the processor;*

p) *at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;*

q) *makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allows for and contributes to audits, including inspections, conducted by the controller or another auditor mandated by the controller.*

r) *The processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other data protection provisions in the Union or domestic law.*

3. Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to above shall be imposed on that other processor by way of a contract or other legal act under Union or domestic law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures.

Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.