Universitatea Transilvania din Brașov

UNIVERSITY SENATE
29 Eroilor Blvd, 500036 - Brașov
tel.: (+40) 268.415.064 | fax: (+40) 268.410.525
presedintele-senatului@unitbv.ro

REGULATIONS
on the natural persons' protection with regard to the personal data processing and on the free movement of these data

CHAPTER I Purpose and scope

Art. 1 Purpose of the Regulations

(1) These Regulations aim to guarantee and protect the natural persons' fundamental rights and freedoms, especially the right to intimate, family and private life, with regard to the personal data processing by Transilvania University of Brașov, hereinafter referred to as UNITBV or controller.
(2) The main purpose of these Regulations is to apply and implement general and clear rules that comply with the provisions of the Regulations no. 679 of 27 April 2016 on the natural persons' protection with regard to the personal data processing and to the free movement of these data, but also on the general principles which underlie this normative act.
(3) These Regulations aim to implement a procedure based on which UNITBV can proceed both to collecting the personal data of all natural persons with whom it will enter into legal relationship, but also to processing such personal data, within the limits in which this processing is absolutely necessary in relation to the activity of UNITBV and for the development of those legal relationships in which UNITBV is a party. The implementation of these Regulations aims to process personal data in full compliance with the legislation in force, without prejudicing the natural persons' fundamental rights and freedoms.

Art. 2 Scope of the Regulations

(1) These Regulations apply to the personal data processing that is made, in full or in part, by automatic means, as well as to the processing by other means than the automatic ones of the personal data which are part of a filing system, or which are intended to be included in such a system.
(2) These Regulations will apply to all departments, compartments, offices and structures that come under the organizational chart of UNITBV, regardless of whether they collect personal data and/or perform personal data processing operations. These Regulations will apply from the date of their entry into force to all members of the academic community and to all third parties with whom UNITBV has legal relationships in general, namely labour, tuition, collaboration, delegation, or any other kind of relationship, throughout their activity resulting from the relationships with UNITBV, as well as subsequently, throughout the legal period during which UNITBV must archive the personal data processing.
(3) From the moment of their entry into force, these Regulations will be brought to the attention of all UNITBV departments, compartments, offices and structures by public display on the institution's website, so that they are known by all employees, collaborators and persons conducting any type of activity involving the legal liability of the controller. Compliance with these Regulations is mandatory and may entail the patrimonial liability of the person who does not abide by them, under the law.

CHAPTER II Terms and principles

Art. 3 Principles governing these Regulations

(1) **Principle of respect for the natural persons' fundamental rights and freedoms**
These Regulations aim for the entire activity of personal data collection and processing to be conducted, regardless of the persons' citizenship or place of residence, in full respect for their fundamental rights and freedoms. These Regulations aim to ensure the achievement of a space of freedom, security and justice with regard to the free movement of personal data.
(2) Among the principles that led to the adoption of these Regulations, by way of example, we mention the compliance with the following principles: respect for private and family life, respect for the right to residence, respect for the freedom of communication, respect for the protection of personal data, respect for the freedom of thought, conscience and religion, the freedom of expression and information, the freedom to conduct a business, respect for the right of access to an effective remedy and to a fair trial.
(3) **Principle of legality** – The Regulations aims to comply with the applicable legal provisions regarding the protection of personal data in the natural persons' case. From its entry into force, any activity involving the processing of personal data will be conducted in full compliance with Regulations no. 679 of 27 April 2016, with subsequent amendments.
(4) **The principle of fairness and transparency** will be complied with by the application of these Regulations, as defined by the Regulations no. 679/2016, with subsequent amendments. The personal data will be collected and processed for well-determined purposes, known from the beginning by their holder. Further processing of these personal data, after the cessation of the legal relationship between the data subject and the controller, will be done for archiving purposes in the public interest, for scientific and/or historical research purposes or for statistical purposes; as this type of initial processing is not considered incompatible with the initial purpose for which the consent was obtained from the data subject.
(5) **Adequate processing, limited to what is necessary** in relation to the purposes for which they are processed, in accordance with the principle of data minimization. These Regulations aim to implement a procedure in which only the data that are necessary for developing the legal relationships in which both the controller and the natural persons are part are collected and processed.
(6) Collection and processing of **accurate personal data,** under the legal provisions. According to these Regulations, the controller will take all necessary steps to ensure that the data collected and processed in full compliance with the law are accurate. In the event that the data are inaccurate or have undergone changes, the controller will take all necessary steps to correct and update the personal data, while the inaccurate ones will be deleted without delay.
(7) **The principle of storage limitation** allows the controller to keep the personal data for the period of time during which their collection and processing are necessary, with a view to fulfilling the purposes for which they were collected and/or processed. Due to the specificity of the controller's activity, after the personal data are no longer necessary for developing the legal relationship under which they were collected, they will be archived for an indefinite period, given that the controller makes an archiving in the public interest, for scientific research purposes and for statistical purposes.
(8) **Principle of integrity and confidentiality.** These Regulations aim to ensure adequate security of personal data against unauthorized or illegal processing, against accidental loss or destruction, by taking appropriate technical or organizational measures.
(9) **Lawfulness of personal data processing.** The personal data will be processed by the controller, based on these Regulations, if one of the following cases occurs:
a) the data subject has consented to the processing of his/her personal data for one or more specific purposes;
b) the processing is necessary in order to execute a contract in which the data subject is a party, or in order to take steps at the data subject's request prior to entering into a contract;

c) the processing is necessary in order to fulfill a legal obligation that rests with the controller;
d) the processing is necessary in order to protect the vital interests of the data subject or of another natural person;
e) the processing is necessary in order to fulfill a task that serves a public interest or that results from the exercise of the public authority with which the controller is vested;

Art. 4 Definition of specific terms

(1) The terms used are defined as established in the Regulations no. 679/2016, with subsequent amendments, on the natural persons' protection with regard to the processing of personal data and to the free movement of these data:
a) **"personal data"** are any information related to an identified or identifiable natural person ("data subject");
An identifiable natural person is a person who can be identified, directly or indirectly, in particular by reference either to an identifier such as a name, an identification number, localization data, an online identifier, or to one or more factors specific to that natural person's physical, physiological, genetic, mental, economic, cultural or social identity;
b) **"processing"** refers to any operation or series of operations made on personal data or personal data sets, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, deletion or destruction;
c) **"restriction of processing"** implies marking stored personal data, with a view to limiting their future processing;
d) **"profiling or creation of profiles"** is any form of automated personal data processing, which consists in the use of personal data to evaluate certain personal aspects related to a natural person, especially in order to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;
e) **"pseudonymization"** means processing of personal data in such a way that they can no longer be assigned to a specific data subject without resorting to additional information, provided that such additional information is stored separately and undergoes technical and organisational measures ensuring that those personal data are not assigned to an identified or identifiable natural person;
f) **"data filing system"** is any structured set of personal data that are accessible according to specific criteria, whether centralized, decentralized or dispersed according to functional or geographic criteria;
g) **"controller"** is the natural or legal person, public authority, agency or other body which, alone or jointly with others, sets the purposes and means of the personal data processing; when the purposes and means of the processing are established by Union law or internal law, the controller or the specific criteria for his/her appointment may be provided for in the Union law or the internal law;
h) **"processor"** is a natural or legal person, public authority, agency or another body which processes personal data on behalf of the controller, based on a contract concluded to that effect;
i) **"recipient"** is the natural or legal person, public authority, agency or any other body to which the personal data are disclosed, whether a third party or not. However, the public authorities to which personal data may be communicated in the framework of a particular survey in accordance with the Union law or Member State law are not considered recipients; the processing of such data by those public authorities complies with the applicable data protection rules according to the purposes of the processing;
j) **"third party"** refers to a natural or legal person, public authority, agency or body other than the data subject, controller, processor and the persons who, under the direct authority of the controller or processor, are authorised to process personal data;
k) **"data subject's consent"** implies any freely given, specific, informed and unambiguous indication of the data subject's wishes by which s/he, by a declaration or by an unequivocal action, agrees that the personal data concerning him/her should be processed;

l) **"personal data breach"** is a breach of security that leads, accidentally or unlawfully, to destruction, loss, alteration, or unauthorized disclosure of the personal data transmitted, stored or otherwise processed, or to unauthorized access to it;
m) **"biometric data"** are the personal data resulting from specific technical processing related to a natural person's physical, physiological or behavioural characteristics, which allow or confirm the unique identification of the person concerned, such as facial images or dactyloscopic data;
n) **"main establishment"** refers to:

1. in the case of a controller headquartered in at least two member states of the EU, the place where its central administration is located, unless the decisions on the purposes and means of the personal data processing are made on other premises of the controller, which premises have the authority to order the implementation of these decisions, in which case the establishment having taken those decisions is considered as the main establishment;
2. in the case of a processor headquartered in at least two member states, the place where his/her central administration is located in the EU; or, if the processor does not have a central administration in the EU, the processor's establishment in the EU where the main processing activities take place, in the context of the activities within one of the processor's establishments, to the extent that it is subject to specific obligations pursuant to this Regulation;

o) **"representative"** is a natural or legal person residing in the EU, appointed in writing by the controller or processor pursuant to art. 27, which represents the controller or processor with regard to their respective obligations under these Regulations;
p) **"enterprise"** is a natural or legal person conducting an economic activity, regardless of its legal form, including partnerships or associations which conduct an economic activity on a regular basis;
q) **"binding corporate rules"** refer to the personal data protection policies to be observed by a controller or processor headquartered on a Member State's territory, as regards the transfers or sets of transfers of personal data to a controller or processor in one or more third countries within a group of companies, or a group of companies involved in a common economic activity;
r) **"supervisory authority"** is the National Supervisory Authority for Personal Data Processing.

CHAPTER III Rules on personal data processing

III.1. General rules

Art. 5 The personal data will be processed in informational systems in compliance with the concerned persons' human rights, fundamental freedoms and dignity, the right to personal data protection, the right to private life and personal identity.

Art. 6 The personal data intended to be processed must be:
a) **processed in good faith** and in accordance with the applicable legal provisions;
b) **collected** for specific, explicit and legitimate purposes; further processing of the personal data for statistical, historical or scientific-research purposes will not be considered incompatible with the data collection purpose if it is carried out in compliance with the provisions of the law, including on the notification to the supervisory authority, as well as in compliance with the guarantees on the personal data processing, as provided for in the rules governing the statistical activity, and the historical or scientific research;
c) **adequate, relevant and not excessive,** by reference to the purpose for which they are collected and subsequently processed;
d) **accurate and, where appropriate, updated;** in this regard, the necessary measures will be taken to ensure that inaccurate or incomplete data in terms of the purpose for which they are collected and for which they will be subsequently processed, are deleted or rectified;
e) **stored** in a form that allows the data subjects' identification strictly over the period of time necessary to

achieve the purposes for which the data are collected and for which they will be further processed; the data storage over a longer period than the one mentioned, for statistical, historical or scientific-research purposes, will be made in compliance with the guarantees on the personal data processing, as provided for in the rules governing these fields, and only for the period necessary to achieve these purposes.

Art. 7 Transilvania University of Brașov, as a controller, has the obligation to comply with the provisions of art. 2 and to ensure the fulfilment of these provisions by the processor.

Art. 8 The personal data can only be processed by the data controller and/or the person authorised by the former, respectively the one employed as a personal-data operator who, through the job description and according to its specificity, works on personal data.

Art. 9 The personal data are processed by the controller and processors exclusively for the purposes for which they were collected.

Art. 10 The personal data, which are adequate, relevant and non-excessive, may only be processed with a view to fulfilling a legitimate interest, and any personal data processing can only be made if the data subject has expressly and unequivocally consented to that processing.

Art. 11 Before expressing consent to personal data processing, the controller shall inform the data subject at least about: the purpose of processing, the method of processing, the duration of storage, the persons whom this restricted information may be provided to, the possibility of consent withdrawal.

Art. 12 The data subject's consent is not required in the following cases:
a) when the processing is necessary in order to executing a contract or pre-contract in which the data subject is a party or in order to take measures, at his/her request, prior to the conclusion of a contract or pre-contract;
b) when the processing is necessary in order to protect the life, physical integrity or health of the data subject or of another threatened person;
c) when the processing is necessary in order to comply with a legal obligation of the controller (including obligations incumbent by ministerial orders);
d) when the processing is necessary in order to enforce measures of public interest or aimed at the exercise of public authority prerogatives with which the operator or the third party to whom the data are disclosed is vested;
e) when the processing is necessary in order to achieve a legitimate interest of the controller or of the third party to whom the data are disclosed, provided that such an interest does not prejudice the data subject's interest or his/her fundamental rights and freedoms;
f) when the processing concerns data obtained from publicly accessible documents, according to the law;
g) when the processing is done exclusively for statistical, historical or scientific research purposes and the data remain anonymous throughout the processing.

Art. 13 The personal data may not be processed for any purposes other than that for which the consent was initially expressed, except for the cases when the data subject's express and unequivocal prior written consent to data processing has been obtained for all purposes deriving from the controller's activity, according to the information made.

Art. 14 (1) Upon completion of the processing operations, unless the data subject has expressly and unequivocally given his/her consent for another destination or for further processing, the personal data will be:
a) destroyed, unless there is a legal obligation for the controller to archive personal data, respectively to

process such data;
b) transferred to another controller, provided that the initial controller guarantees that further processing has similar purposes to those for which the processing was originally done;
c) rendered anonymous and exclusively stored for statistical, historical or scientific-research purposes.
(2 In the case of the processing operations made under the conditions provided for in art. 12 para. (1) lit. c) or d) of the EU Regulations no. 679/2016, the controller may store personal data for the period of time necessary to achieve the specific purposes pursued, provided that appropriate measures are ensured to protect them, after which s/he will proceed to their destruction if the legal provisions on keeping archives are not applicable.

Art. 15 The data subject may withdraw his/her consent to the personal data processing at any time, which will take effect from the date of processing the express request for withdrawal of consent. The withdrawal of consent does not affect the lawfulness of the consent-based processing, prior to its withdrawal; however, the data subject shall be notified that one of the effects of his/her consent withdrawal will result in the termination of the legal relationship with the controller, including expulsion in the case of students, without being imputable to the controller.

Art. 16 General rules on data processing:
(1) The personal data of the University's students or employees will be transmitted both inside and outside the institution, taking all necessary measures to protect the personal data according to these Regulations.
(2) If the data are requested by other institutions: tax authorities, banks, RATBV, and more, by email, they shall be transmitted only to the email address of the institution notified to the controller in this regard, and only by the controller's employee authorised for this transfer, and only for the purpose of the necessary processing.
When personal data are requested, the person authorised for this transfer must verify whether the applicant has the right to receive that information.
(3) The IT Office will develop a set of rules on ensuring the integrity of the data in use, in transit and in stationary mode, and will monitor their application on the University's IT equipment containing personal data, used equipment, under any legal regime, to carry out the institution's activities.
The University's community members shall implement the measures established by the IT Office.

Art. 17 Special rules
(1) The processing of personal data related to racial or ethnic origin, to political, religious, philosophical or similar beliefs, to trade union membership, as well as of personal data related to health or sex life is prohibited.
(2) The provisions of para. (1) do not apply in the following cases:
a) when the data subject has expressly and unequivocally given his/her consent to such processing;
b) when the processing is necessary in order to meet the controller's obligations or specific rights in the field of labour law, in compliance with the guarantees prescribed by law; The processed data may be disclosed to a third party only if the controller is legally bound in this regard or if the data subject has expressly consented to such disclosure;
c) when the processing is necessary in order to protect the life, physical integrity or health of the data subject or of another person, if the data subject is physically or legally incapable of giving his/her consent;
d) when the processing is made, within its legitimate activities, by a foundation, association or any other non-profit organization with a specific political, philosophical, religious or trade-union purpose, provided that the data subject is a member of this organization or maintains with it as a relationship regarding the specificity of the organization's activity, and that the data are not disclosed to third parties without the data subject's consent;
e) when the processing refers to data manifestly made public by the data subject;

f) when the processing is necessary in order to ascertain, exercise or defend a right in court;
g) when the processing is necessary for the purposes of preventive medicine, medical diagnosis, provided that such data are processed by or under the supervision of a health professional subject to professional secrecy, or by or under the supervision of another person subject to an equivalent obligation in terms of secrecy;
h) when the law expressly stipulates this in order to protect an important public interest, provided that the processing is made in compliance with the data subject's rights and the other guarantees prescribed by this law.
(3) The provisions of para. (2) shall not prejudice the legal provisions governing the obligation of the public authorities to respect and protect intimate, family and private life.

Art. 18 The social security number or other personal data having an identification function of general applicability may be processed only if:
a) the data subject has expressly given his/her consent;
b) the processing is expressly provided for by a legal provision.

Art. 19 (1) The processing of the social-security number or of other personal data having an identification function of general applicability does not apply to health data processing in the following cases:
a) if the processing is necessary for the protection of public health;
b) if the processing is necessary in order to prevent an imminent danger, a criminal offence or the outcome of such an offence from occurring, or to remove the detrimental consequences of such an offence.
(2) The health data may be processed only by, or under the supervision of a health professional, subject to professional secrecy, unless the data subject has given his/her consent in writing and unequivocally, and as long this consent has not been withdrawn, as well as unless the processing is necessary in order to prevent an imminent danger, a criminal offence or the outcome of such an offence from occurring, or to remove the detrimental consequences of such an offence.
3. The personal health data may be collected only from the data subject. By way of exception, these data may be collected from other sources only to the extent that it is necessary in order not to compromise the purposes of the processing, and the data subject does not want or cannot provide them.

Art. 20 The personal data related to the perpetration of offences by the data subject, or to criminal convictions, safety measures, and administrative or civil sanctions applied to the data subject may only be processed by or under the control of the public authorities, within the limits of their powers conferred by law and under the conditions established by the special laws that regulate these matters.

CHAPTER IV The data subject's rights regarding the personal data processing

Art. 21 The data subject's right to information

(1) If the personal data are obtained directly from the data subject, UNITBV as a controller is obliged to provide the data subject with at least the following information, unless that person already has that information:
a) the identity and contact details of the controller and, where applicable, of the processor;
b) the contact details of the data protection officer, where applicable;
c) the purpose for which the data are processed and the legal basis of the processing;
d) if the processing is made under the provisions of art. 6 para. 1 lett. f) in the EU Regulations 679/2016, the legitimate interests pursued by the controller or by a third party;
c) additional information, such as: data recipients or categories of data recipients; whether the provision of all required data is mandatory, and the consequences of the refusal to provide them; the existence of the rights provided for in this law for the data subject, in particular the right of access, intervention on the data and

opposition, as well as the conditions under which they can be exercised;
d) any other information the provision of which is required by orders of the authorities, taking into account the specifics of the processing.
(2) If the data are not obtained directly from the data subject, the controller shall, at the time of data collection or, if disclosure to third parties is intended, at the latest by the time of the first disclosure, provide the data subject with at least the following information, unless the data subject already possesses this information:
(a) the identity of the controller and his/her representative, where applicable;
b) the purpose for which the data is processed;
c) additional information, such as: the categories of data concerned, the data recipients or categories of data recipients, the existence of the rights provided for in this law for the data subject, in particular the right of access, intervention on the data and opposition, as well as the conditions under which they can be exercised;
d) any other information the provision of which is required by orders of the authorities, taking into account the specifics of the processing.
(3) The provisions of para. (2) do not apply where the data processing is made exclusively for journalistic, literary or artistic purposes, if their application would give clues to the sources of information.
(4) The provisions of para. (2) do not apply if the data processing is made for statistical, historical or scientific research purposes, or in any other situations where the provision of such information proves impossible or would involve a disproportionate effort compared to the legitimate interest that could be harmed, as well as in situations where the recording or disclosure of the data is expressly provided for in the law.

Art. 22 The data subject's right to information if the personal data have not been obtained from the data subject
(1) If the personal data are not obtained directly from the data subject, UNITBV as a controller shall provide the data subject with at least the following information, unless that person already possesses that information:
a) the identity and contact details of the controller and, where applicable, of the legal representative;
b) the contact details of the data protection officer, where applicable;
c) the purpose for which the data are processed and the legal basis of the processing;
d) the categories of personal data intended to be processed;
e) recipients or categories of recipients of the personal data;
f) where applicable, the controller's intention to transfer the data to a recipient in a third country or to an international organisation, and the existence or absence of a decision of the Committee on the adequacy or, in the case of the transfers referred to in art. 46 or art. 47, respectively art. 49 para. 1 subpara. II of the EU Regulations 679/2016, a reference to the adequate or appropriate guarantees and to the means of obtaining a copy, where they have been made available;
(2) In addition to the information referred to in para. (1), the controller shall, at the time of the data processing or, if disclosure to third parties is intended, at the latest by the moment of the first disclosure, provide the data subject with at least the following information, unless the data subject already possesses that information, with a view to ensuring fair and transparent processing:
a) the period for which the personal data will be stored; or, if this is not possible, the criteria used to establish such a period;
b) if the processing is made in accordance with art. 6 para. 1 lett. (f) of the EU Regulations 679/2016, the legitimate interests pursued by the controller or by a third party;
c) the existence of the right to request from the controller, with regard to the personal data referring to the data subject, access to them, rectification or deletion thereof, or restriction of processing and the right to oppose processing, as well as the right to data portability;
d) when the processing is based on art. 6 para. (1) lett. (a) or on art. 9 para. (2) let. (a) of the EU Regulations

679/2016, the existence of the right to withdraw consent at any time, without affecting the lawfulness of the processing made on the basis of consent before its withdrawal;
e) the right to lodge a complaint with a supervisory authority;
f) the source in which the personal data originate; and, if applicable, whether they come from publicly available sources;
g) the existence of an automated decision-making process, including the creation of profiles, referred to in art. 22 para. (1) and (4), as well as, at least in those cases, meaningful information on the logic used, and on the significance and envisaged consequences of such a processing for the data subject;
(3) The controller provides the information referred to in para. (1) and (2):
a) within a reasonable time after obtaining the personal data, but not exceeding one month, considering 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 it is intended to disclose the personal data to another recipient, at the latest on the date they are first disclosed.
(4) In case the controller intends to further process the personal data for a purpose other than that for which they were obtained on the basis of consent, the controller shall, prior to such further processing, provide the data subject with information on that other purpose and any relevant additional information in accordance with para. (2).
(5) Paragraphs (1) to (4) shall not apply if and to the extent that:
a) the data subject already has that information;
b) the provision of such information proves impossible or would involve disproportionate efforts, in particular in the case of the processing for archiving purposes in the public interest, for scientific or historical research purposes, or for statistical purposes, subject to the conditions and guarantees provided for in art. 89 para. (1) of the EU Regulations 679/2016, or to the extent that the obligation referred to in para. (1) of this article is likely to render impossible or to severely affect achieving the objectives of that processing. In such cases, the controller shall take appropriate measures to protect the data subject's rights, freedoms and legitimate interests, including making the information publicly available;
c) obtaining or disclosing the data is expressly provided for in the Union law or the internal law under which the operator falls and which sets out adequate measures to protect the data subject's legitimate interests; or
d) if the personal data must remain confidential under a statutory obligation of professional secrecy governed by the Union law or Member State law, including a statutory obligation of secrecy.

Art. 23 The data subject's right of access
(1) The data subject has the right to obtain from the controller a confirmation as to whether or not personal data concerning him/her are being processed; and, if so, access to those data and to the following information:
a) the purposes of the processing;
b) the categories of personal data concerned;
c) the recipients or categories of recipients to whom the personal data have been or are to be disclosed, in particular recipients in third countries or international organisations;
d) where possible, the period for which the personal data are expected to be stored; or, if this is not possible, the criteria used to establish that period;
e) the right to request the controller to rectify or delete the personal data, or to restrict the processing of the personal data relating to the data subject, or the right to oppose the processing;
f) the right to lodge a complaint with a supervisory authority;
g) if the personal data are not collected from the data subject, any available information as to their source;
h) the existence of an automated decision-making process, including the creation of profiles, referred to in

art. 22 para. (1) and (4), as well as, at least in those cases, relevant information on the logic used, as well as on the significance and envisaged consequences of such processing for the data subject.
(2) If the personal data are transferred to a third country or an international organisation, the data subject has the right to be informed of the appropriate guarantees pursuant to art. 46 of the EU Regulations 679/2016 on the transfer.
(3) The controller shall provide a copy of the personal data that undergo processing. For any other copies required by the data subject, the controller may charge a reasonable fee based on the administrative costs. If the data subject submits the application in electronic format, and unless the data subject required a different format, the information is provided in a currently used electronic format.
4. The right to obtain a copy referred to in para. 3 shall not prejudice the rights and freedoms of others.

Art. 24 The right to request data rectification
The data subject has the right to obtain from the controller, without undue delay, the rectification of inaccurate personal data concerning him/her. Taking into account the purposes for which the data have been processed, the data subject is entitled to have his/her incomplete personal data filled in, including by means of providing a supplementary statement.

Art. 25 The right to have one's data deleted from the controller's records
1. The data subject is entitled to have the controller delete the personal data concerning him/her without undue delay, and the controller is bound to delete the personal data without undue delay where one of the following grounds applies:
a) the personal data are no longer necessary to fulfill the purposes for which they were collected or processed;
b) the data subject withdraws his/her consent on the basis of which the processing takes place, in accordance with art. 6 para. (1) lett. (a) or art. 9 para. (2) lett. (a) of the EU Regulation, and there is no other legal basis for the processing;
c) the data subject opposes the processing pursuant to art. 28 para. (1) hereof, and there are no overriding legitimate grounds for the processing, or the data subject opposes the processing pursuant to art. 28 para. (2) hereof;
d) the personal data have been processed unlawfully;
e) the personal data must be deleted for compliance with a legal obligation to which the controller is subject under the Union law or the Member State law to which the controller is subject;
f) the personal data have been collected in relation to the provision of the informational society-related services referred to in art. 8 para. (1) of the EU Regulations 679/2016.
(2) If the controller has made the personal data public and is bound, pursuant to para. (1), to delete them, the controller shall, taking into account the available technology and the cost of implementation, take reasonable measures, including technical measures, to inform the personal data processing controllers that the data subject concerned has requested those controllers to delete any links to, as well as copies or replications of those personal data.
(3) Paragraphs (1) and (2) do not apply insofar as the processing is necessary:
a) to exercise the right to freedom of expression and information;
b) to comply with a legal obligation that makes provision for the processing under the Union law or the Member State law to which the controller is subject, or to perform a task in the public interest or within the exercise of an official authority which the controller is vested with;
c) for reasons of public interest in the field of public health, in accordance with art. 9 para. (2) lett. (h) and (i), and with art. 9 para. (3) of the EU Regulations 679/2016;
d) for archiving purposes in the public interest, for scientific or historical research purposes, as well as for statistical purposes, in accordance with art. 89 para. (1) of the EU Regulations 679/2016, to the extent that

the right referred to in para. (1) is likely to render impossible or to severely impact achieving the objectives of that processing; or
e) to establish, exercise or defend a right in court.

Art. 26 Right to restrict the data processing
1. The data subject has the right to obtain from the controller the restriction of processing where one of the following cases applies:
a) the data accuracy is contested by the data subject, for a period allowing the controller to verify the accuracy of the data;
b) the processing is unlawful, and the data subject opposes to the deletion of the personal data, requesting instead the restriction of their use;
c) the controller no longer needs the personal data for processing purposes, but the data subject requests them in order to establish, exercise or defend a right in court; or
d) the data subject has opposed the processing in accordance with art. 28 para. (1) hereof, pending the verification whether the legitimate rights of the controller prevail over those of the data subject.
(2) If the processing has been restricted pursuant to para. (1), such personal data may, except for storage, be processed only with the data subject's consent, or for establishing, exercising or defending a right in court, or for protecting the rights of another natural or legal person, or for reasons of important public interest to the Union or to a Member State.
3. A data subject who has obtained the restriction of processing under para. (1) will be informed by the controller before the restriction of the processing is lifted.
4. The controller will notify each recipient to whom the personal data have been disclosed of any rectification or deletion of his/her personal data, or of any processing restriction made in accordance with art. 24, 25 para. (1), and 26 para. (1) hereof, unless this proves impossible or involves disproportionate efforts. The controller informs the data subject of those recipients if the data subject requests this.

Art. 27 Right to data portability
(1) The data subject has the right to receive the personal data concerning him/her which s/he has provided to the controller in a structured, commonly used and machine-readable format, and has the right to transmit such data to another controller without hindrance from the controller to whom the personal data have been provided, where:
a) the processing is based on consent, pursuant to art. 6 para. (1) lett. (a), or art. 9 para. (2) lett. (a) of the EU Regulations 679/2016, or on a contract, pursuant to art. 6 para. (1) lett. (b) of the EU Regulations 679/2018; and
b) the processing is made by automated means.
2. In exercising his/her right to data portability pursuant to para. (1), the data subject is entitled to have his/her personal data transmitted directly from one controller to another, where technically feasible.
3. The exercise of the right referred to in para. (1) of this article does not prejudice art. (25) hereof. That right does not apply to the processing necessary for performing a task in the public interest or in the exercise of an official authority which the operator is vested with.

Art. 28 Right to object
(1) At any time, the data subject has the right to object to the processing, on grounds relating to his/her particular situation, pursuant to art. 6 para. (1) lett. (e) or (f), or to art. 6 para. (1) of the EU Regulations 679/2016, of the personal data concerning him/her, including the creation of profiles based on those provisions.
The controller no longer processes personal data, unless the operator proves that it has legitimate and compelling reasons which justify the processing and which prevail over the data subject's interests, rights and freedoms, or that the purpose is to establish, exercise or defend a right in court.

(2) When the personal data processing is aimed at direct marketing, the data subject has the right to object at any time to the processing of the personal data concerning him/her, including the creation of profiles, insofar as it is related to that direct marketing.
(3) If the data subject objects to the processing for direct marketing purposes, the personal data will no longer be processed for that purpose.
(4) At the latest upon the first communication with the data subject, the right referred to in para. (1) and (2) shall be explicitly brought to the data subject's attention and be presented clearly and separately from any other information.
(5) In the context of using the informational society services and notwithstanding the Directive 2002/58/EC, the data subject concerned may exercise his/her right to object, by automated means using technical specifications.
(6) Where the personal data are processed for scientific or historical research purposes, or for statistical purposes, in accordance with article 89 para. (1) of the EU Regulations 679/2016, the data subject, for reasons related to his/her particular situation, has the right to object to the processing of the personal data concerning him/her, unless that processing is necessary in order to perform a task for reasons of public interest.

Art. 29 Automated individual decision-making, including the creation of profiles
(1) The data subject has the right not to be under a decision based solely on automated processing, including the creation of profiles, which produces legal effects regarding him/her or similarly affects him/her to a significant extent.
(2) Para. (1) does not apply where the decision:
a) is necessary to conclude or execute a contract between the data subject and a data controller;
b) is authorised by Union law or the Member State law which is applicable to the controller, and which also sets out adequate measures to protect the data subject's rights, freedoms and legitimate interests; or
c) is based on the data subject's explicit consent.
(3) In the cases referred to in para. 2 lett. (a) and (c), the data controller shall implement appropriate measures to protect the data subject's rights, freedoms and legitimate interests, at least the right to obtain human intervention from the controller, to express his/her point of view, and to contest the decision.
(4) The decisions referred to in para. (2) are not based on the special categories of personal data referred to in art. 9 para. (1) of the EU Regulations 679/2016, unless art. (2) lett. (a) or (g) applies, and unless appropriate measures have been put in place to protect the data subject's rights, freedoms and legitimate interests.

CHAPTER V Measures to ensure the confidentiality and security of personal data processing

Art. 30 (1) In order to obtain access to personal data, the users of the controller (the employees designated for data collection and/or processing, and the employees who, according to their job description, have work assignments of personal data processing) must log in to the University's IT systems. The login to the University's IT systems requires entering one's unique and non-transferable authentication credentials acquired following the enrollment and the electronic identity management process, governed by the applicable security policies.
(2) The controller shall ensure, with a view to guaranteeing the security of the processing, that each user has his/her own identification code (user name). The same identification code is never assigned to multiple users, and it cannot be shared by multiple persons.
The identification codes (or user accounts) are deactivated and destroyed after a prior check upon completion of studies, in the students' case, respectively upon termination of the relationship with UNITBV.
(3) Any user who receives an identification code and a means of authentication is bound, by the job description, to keep them confidential, and is liable in this regard to the controller.

V.1. Processing of the students' personal data

Art. 31 (1) The University processes the following data of the students enrolled at UNITBV, regardless of the course of study and/or study programme, including the temporary mobility-based students' data:

A) Surname and forename;
B) Contact details: B1): home address, B2) SSN, B3) email account and/or phone, B4) series and number of the identity card/passport/residence permit
C) Special medical situations (diseases, disabilities);
D) Social situations (orphans, in foster care, from orphanages);
E) Data on the membership in a religious cult;
F) Photographs;
G) School results (grades, special situations: re-enrollment, resumption of studies, extension of tuition, transfers, etc.);
H) Income per family member.

(2.1) Purpose of data processing:

- admission lists;
- scholarships;
- grants;
- for the following situations: the graduates' ranking (written on the diploma supplement), the ranking for filling in the semester or annual state budgeted places, expulsions;
- internal and external temporary mobility;
- accommodations;
- awards;
- traineeship;
- orphanages;
- different European projects;
- private scholarships granted to students.

(2.2) The personal data referred to in para. (1) lett. A) and B), collected and processed, are also found in the database AGSIS, RMU, Liberty, in the admission application, on the intranet, in the academic records, respectively the data referred to in para. (1) lett. A) and B3) for the academic teaching personnel's records (agendas), and the data referred to in para. 1 lett. A) for the website of each faculty within the University.

(3) The data referred to in para. (1) are processed as a matter of priority at faculty level, the processing being coordinated by the faculty's secretary in chief; and at university level, the processing continues at the level of the institution, according to the purpose referred to in para. (2) of this article. At institutional level, the processing is coordinated by the employee assigned through the job description or work duties (including duties delegated through regulations or by the UNITBV management).

(4) Students give their consent to the processing by UNITBV of the data referred to in para. (1) at the time of their enrolment, by signing the tuition contract, as they are data necessary for the proper conduct of the tuition relationship. The student's withdrawal of consent to personal data processing entails his/her expulsion, either from the date of filing such a request, or as a consequence of exercising the right to data deletion, pursuant to art. 25 hereof; the processing made up to that moment is not affected.

V.2. Processing of the teaching personnel's personal data

Art. 32 (1) The University, in line with its scope of activity and as an employer, processes the academic personnel's following types of personal data:

(A) Surname and forename;
(B) Contact details: home address, SSN, email, telephone;

(C) Special medical situations (diseases, disabilities);
(D) Family situations (personal data: children and/or spouse);
(E) Membership in a religious cult;
(F) Photographs.

(2) The academic personnel's contact details, as they are also personal data, must not be disclosed to students or third parties without the former's express consent, unless the communication of personal data is provided for in legal and/or regulatory-administrative provisions.

(3) The academic teaching personnel gives their consent to the data processing by UNITBV as referred to in para. (1) at the time of employment, even from the selection phase for employment, by signing the individual labour contract and the job description, as they are data necessary for the proper conduct of the employment relationship. The withdrawal of consent to the personal data processing entails the cessation of the employment relationship and the termination of the individual labour contract, from the date of filing such a request or after exercising the right to data deletion according to art. 25 hereof; the processing carried out up to that moment is not affected.

(4) The academic teaching personnel's personal data are processed as a matter of priority at university level through the Human Resources Service. The processing is coordinated by the Head of Service, on a confidential basis, and by the other employees within the aforementioned department, or by structures nominated through decisions of the Executive Board.

At faculty level, the personal data collection and processing is coordinated by the Dean and/or Director of department and faculty chief secretary.

CHAPTER VI Organization and operation of the University's Data Protection Compartment

Art. 33 (1) The Data Protection Compartment is a support structure that ensures the coordination and implementation of the University's policies on the security of the personal data processed at the University's level.

(2) The Data Protection Compartment is part of the structure of the Vice-Rectorate for Public Relations, and conducts its activity according to the applicable legislation.

(3) Within the Data Protection Compartment, the activities are monitored and coordinated by a DPO (Data Protection Officer according to the EU Regulations 679/2016), which is an auxiliary teaching position with management powers, as well as with specific duties and responsibilities in processing and protecting the personal data managed at the University's level.

(4) The activities conducted by DPO are supported logistically, consultatively and at the level of regulation of the institutional policy in the field by the Committee on the Implementation of Personal Data Protection Policies, a committee appointed by Rector's decision, at the proposal and with the approval of the Executive Board. The Committee is chaired by a coordinator, tenured professor within the University, appointed by the Executive Board. The mandate of the Committee is valid throughout the term of office of the management bodies, starting from the date of approval of the Committee by the newly invested Executive Board, respectively until the date of appointment of the Committee by the newly invested Executive Board.

Art. 34 (1) The Data Protection Compartment has as its main objective the implementation of institutional measures and policies regarding the personal data protection in the institution's processing.

(2) The Coordinator of the Compartment, who also fills the position of DPO (Data Protection Officer), has the following duties and responsibilities, according to the job description:

a) to ensure the proper conduct of the activities within the Data Protection Compartment under optimal conditions;

b) to answer for the correct, transparent and equitable implementation of the provisions in the legislation on the personal data protection and on ensuring the security measures regarding the processing, transfer and archiving of the personal data at the institutional level;

c) to answer for the verification, at the level of the University's all structures, departments, compartments and offices, of the security measures regarding the protection of the personal data processing, as well as for the proper conduct of the personal data processing at the level of the University and/or faculties, in compliance with the technical security measures, as well as with the applicable legal provisions;
d) to ensure, together with the Committee on the Implementation of Personal Data Protection Policies, the adaptation of all internal provisions that have a bearing on the personal data processing, as well as the adoption of all necessary instruments, including of the internal documents, in order to ensure the collection, processing and archiving of the personal data;
e) to ensure, together with the Committee on the Implementation of Personal Data Protection Policies, the mapping of the personal data at the institutional level, on a periodical basis;
f) to compulsorily endorse the answers and/or to answer the requests of third parties regarding the communication of the academic community members' personal data. In this regard, all structures, departments/compartments and/or offices at the level of which requests for personal data communication are registered/ communicated shall be addressed to DPO as regards the registered application and will collaborate with him/her in formulating the possible answer;
g) periodically and whenever legislative changes in the personal data regime occur, to train the institution's employees who have in their job description, respectively as duties, the collection, processing, transfer and archiving of personal data;
h) to answer to the authorities with duties in supervising the personal data processing for any complaint regarding the University's activity and to prepare the reports and/or mail provided for in the legislation on personal data protection.

Art. 35 The organizational structure of the Data Protection Compartment (number and duties of its positions) meets the University's strategy and needs, being established according to the internal regulations and applicable legislation.

Art. 36 The University's employees who, through their job description, respectively through their job duties, have to perform processing operations (including transfer and archiving) of personal data also have the obligation to observe and ensure the confidentiality of the data and operations with these data; and their legal liability is involved in cases where the University is held liable for infringing the natural persons' rights regarding personal data processing.

CHAPTER VII Anonymization and cross-border transfer of personal data in the University

Art. 37 Every data subject is entitled, upon request and free of charge:
a) to have the controller rectify, update, block or delete the data the processing of which is not in accordance with the law, especially of the incomplete or inaccurate data, or as the case may be,
b) to have the controller turn the data the processing of which is not in accordance with the law, into anonymous data (the latter are data which, due to their origin or specific way of processing, cannot be associated with an identified or identifiable person); in cases where the anonymization operation is impossible, the person concerned will be notified of the reasons why the transformation into anonymous data is not possible.

Art. 38 In order to exercise this right, the data subject shall submit to the controller a written, dated and signed application.

Art. 39 The controller shall communicate the measures taken following the data subject's application within 30 days from the date of receipt thereof.

Art. 40 Each case of request for access to the data subject's personal data contained in his/her personal files, made by a subject other than the data subject, must be formulated in writing, signed, dated and analysed in detail by the controller through the coordinator of the Data Protection Compartment, in order to identify:

a) the purpose for which the availability of these data is requested, and whether or not this purpose is related to the purposes for which the personal data were collected;

b) the volume and categories of personal data to which access is requested;

c) the conditions under which the personal data will be kept and the terms for which these data are required;

d) the legal framework underlying the applicant's request for access to these data;

e) the personal data subject's consent for the transmission of the information contained in his/her personal file;

f) a legal basis allowing access to or making available to third parties the information containing personal data, failing the data subject's consent.

Art. 41 The information on the data subject's personal data shall be provided to the interested person in writing and within a maximum of 30 days, under the conditions established by the legislation in force.

Art. 42 If the need arises for the cross-border transfer of certain personal data regarding persons with whom the University has or had contractual legal relationships based on the person's consent to the processing of his/her personal data, the office/compartment/department/employee who must transfer personal data in the name and on behalf of UNITBV shall address the Data Protection Compartment in order to analyse and establish together the nature of the personal data, the purpose of the processing and the country to which the data are transferred (country of destination) as well as the guarantees on the protection of the personal data to be transferred.

CHAPTER VIII Final and transitional provisions

Art. 43 These Regulations complement the internal regulatory provisions and the instructions/procedures in which personal data-related operations and/or actions conducted for the purpose and in line with the institution's activities are regulated and/or described.

Art. 44 After the adoption and implementation of these Regulations, within a maximum of 6 (six) months, the Data Protection Compartment will ensure, together with the specialized committees of the Senate and the Quality Assurance Office, the adaptation of all standard forms and documents, respectively of the instructions that have personal data operations as their object.

Art. 45 After the adoption and implementation of these Regulations, within a maximum of 6 (six) months, the IT Office will develop the set of instructions that have the operations with personal data referred to in Article 16 as their object.

Art. 46 The institutional policy regarding the information that is publicly displayed on the website of the institution, respectively of the faculties, is implemented under the conditions of compliance with the legislation on the regime of personal data by the faculty officers for the website, respectively by the Compartment of Communications.

These Regulations were approved in the meeting of the Senate of Transilvania University of Brașov on 24.07.2024.

Prof. Eng. Mircea Horia Țierean, PhD
President of the University Senate

APPENDIX 1

Minimum Requirements for the Personal Data Processing

This appendix contains minimum security requirements for personal data processing and must underlie the adoption and implementation by the UNITBV controller of the technical and organizational measures necessary for maintaining the confidentiality and integrity of the personal data, in full compliance with the provisions of the Regulations no. 679/27 April 2016, in force as of 25 May 2018.
The minimum security requirements for the personal data processing cover the following aspects:

1. User identification and authentication

User is any person acting under the authority of the controller, processor or representative, with acknowledged right of access to personal databases.
The users, in order to gain access to a personal database, must identify themselves. The identification can be done by several methods, such as: entering the keyboard identification code (a string of characters), using a barcode card, using a smart card or a magnetic card.
Each user has his/her own identification code. Multiple users must never have the same identification code.
Identification codes (or user accounts) not used for a longer period (e.g. for a minimum of one year) must be deactivated and destroyed after having been previously verified the controller. The period after which the codes must be deactivated and destroyed is established by the controller together with the members of the IT Office.
Any user account has an authentication method. Authentication can be done by entering a password.
Passwords are strings of characters. The longer the string, the harder it is to break the password. When entering passwords, they should not be clearly displayed on the monitor. The passwords must be changed periodically according to the security policies of the entity (controller or processor) and must contain a combination of uppercase and lowercase characters, numbers and punctuation marks, in order to be harder to find out/detect. Periodic change of passwords is recommended at a period of time to be established by the controller with the IT Office.
The controller must request the development of an IT system that automatically denies a user's access after 5 wrong password inputs. Only the IT Office can unlock access to the blocked account after identifying the user by any necessary means, leading to the conclusion that the applicant is identical to the user, under the terms of this Regulations and this Appendix.
Any user who receives an identification code and an authentication means needs to keep their confidentiality and answer to the controller in this regard.
The IT Office will establish its own procedure for administering and managing user accounts, the procedure in case of a blocked account as a result of entering a wrong identification code and password 5 times, etc.
The controller authorises only certain users within the IT Office to revoke or suspend an identification and authentication code, in situations such as: their user has resigned or has been fired, has terminated his/her contract, has changed his/her name, has been transferred to another department/compartment/office, and his/her new tasks do not imply access to personal data, has abused the codes received, will be absent for a long period of time established by the entity, and other.
User access to made manually personal databases will be granted after the user has signed a declaration according to which s/he has taken note of the provisions of these Regulations, of his/her ghts and obligations, given that consulting personal databases involves processing under the law.

2. Type of access

Users must access only the personal data necessary to perform their job duties. For this, the controller must establish the types of access according to functionality (such as: administration, input, processing, saving,

consultation, etc.) and to the actions applied to personal data (such as: writing, reading, deletion), as well as the procedures regarding these types of access.
Programmers of personal data processing systems will not have access to the personal data. The controller will allow the programmers' access to personal data after they have been turned into anonymous data.
The compartment providing technical support may have access to personal data for solving exceptional cases.
For user training or making presentations, anonymous data will be used. The employees teaching the training courses will resort to personal data during their own training.
The controller will establish the strict ways in which personal data will be destroyed. Authorization for this personal data processing must be limited to a few users within the IT Office.

3. Data collection

The personal data will be collected starting on 25 May 2018, provided that the data subject has given his/her written consent, as stipulated in art. 7 of Regulations no. 679/2016. The personal data will be collected by all users who have job duties in this regard, who are part of legally established committees at the level of the controller, only after these Regulations has been brought to their attention.
Any modification of the personal data can only be made by users who have specific duties in this regard, and only if the initially collected data are inaccurate or have undergone changes from the date of their collection until the date on which their correction / modification is made.
The controller will take measures for the informational system to record who made the change, as well as the date and time of the change.

4. Creation of backup copies

The controller will establish the period of time at which the backup copies of the personal databases will be made, as well as the programmes used for automated processing. The users who make these backups will be appointed by the controller, in a limited number. The backups will be stored in other rooms, in sealed metal cabinets, and, if possible, even rooms in another building.
The controller will ensure that access to backups is monitored.

5. Access terminals and computers

Computers and other access terminals will be installed in restricted-access rooms. If these conditions cannot be provided, the computers will be placed in lockable rooms, or measures will be taken for the access to computers to be made by means of keys or magnetic cards.
If personal data appear on the screen over which no action is taken for a period of time set by the controller, the working session must be closed automatically. The length of this period is established depending on the operations to be performed.
The access terminals used in the relationship with the public, on which personal data appear, will be placed so that they cannot be seen by the public; and, after a short period set by the controller, during which no action is taken over them, they must be hidden.

6. Access files

The controller is obliged to take measures for any access to the personal database to be recorded in an access file (called log for automatic processing) or in a register for manual processing of personal data, established by the controller. The information entered in the access file or in the register will be:
- identification code (user name for manual personal databases);
- name of the accessed file (sheet);
- number of records;
- type of access;
- the code of the operation performed or computer programme used;

- date of access (year, month, day);
- time (hour, minute, second).

For automatic processing, this information will be stored in a general access file or in separate files for each user. Any unauthorized access attempt will also be recorded.

The controller is obliged to keep the access files for at least 2 years, in order to be used as evidence in case of investigations. If the investigations are prolonged, these files will be kept for as long as deemed necessary.

The access files must make it possible for the controller or processor to identify the persons who have accessed personal data without a specific reason, with a view to imposing sanctions or referring the matter to the competent authorities.

7. Telecommunications systems

The controller is obliged to periodically check the authentications and types of access in order to detect malfunctions in the use of telecommunications systems.

Controllers are obliged to design the telecommunications system so that the personal data cannot be intercepted or transmitted from anyplace. If the telecommunications system cannot be secured in this way, the controller shall impose the method of encryption for the transmission of personal data.

Only strictly necessary personal data will be transmitted through telecommunications systems.

8. Staff training

After the approval and implementation of these Regulations, the controller must ensure the transmission thereof at institutional level, so that all users are notified of its content. Moreover, the controller will notify users about the provisions of the Regulations no. 679/2016, and about all users' obligations to abide by these legal provisions.

The users who have access to personal data and who will perform processing activities on these data will be trained by the controller in terms of their confidentiality, and will be warned by messages appearing on the monitors during this activity. Users must close their work session when leaving their workplace.

9. Computer use

In order to maintain the security of personal data processing (especially against computer viruses), the controller will take measures:

a) to prohibit the users' working with computer programmes coming from external or dubious sources;

b) to inform users about the danger of computer viruses;

c) to implement automatic virus removal systems and ensure the security of IT systems;

d) to deactivate, as much as possible, the "Print screen" key when personal data are displayed on the monitor, thus prohibiting their printing;

e) to use computers and institutional email addresses only for the fulfilment of the work duties.

10. Data printing

Personal data will be printed only by the users authorised for this operation by the controller and only when this is absolutely necessary. The controller together with each department/ compartment/ office will establish specific internal procedures for the use and destruction of these materials.

Each entity will approve its own security system, taking into account these minimum security requirements for personal data processing; and, depending on the importance of the processed personal data, it will impose additional security measures.

a) students

Minimum Mandatory Content of the Declaration of Consent to Personal Data Processing

Declaration of Consent to Personal Data Processing within the Tuition Relationship

A. Information

Transilvania University of Braşov, headquartered in Braşov, 29 Eroilor Avenue, Braşov county, tel. 0268 410525/0268 413000, represented by Rector Prof. Eng. Ioan Vasile ABRUDAN, PhD, is a personal data controller for the stated purpose "education and culture", "candidates' record in the admission/graduation exam", "undergraduate, graduate and doctoral students' record".

In accordance with the provisions of the EU Regulations no.2016/679, Transilvania University of Braşov processes *personal data*, on legal grounds and under conditions that ensure the security, confidentiality and respect for the data subjects' rights.

Personal data are any information about an identified or identifiable natural person. This information may include, but is not limited to name, address, social security number, phone number, and any other necessary information related to the students' individualization and record, including the institutional email address assigned at the time of enrollment.

The personal data may be communicated between Transilvania University of Braşov and other institutions or public bodies in the field of education, which may use the information for purposes of information and culture, as well as for the students' record, according to the National Education Law no. 1/2011.

Your data are necessary for the compilation of the personal student file, for the implementation of the contract of academic studies and for the proper conduct of the legal relationship of tuition, with its related education and research activities, including examinations/evaluations, internal and international mobilities, both temporary and definitive, granting of scholarships and other forms of support, granting of student facilities, provision of accommodation, where applicable, organization of competitions, student camps and other events, issuance and record-keeping of study documents, graduates' record. At the same time, upon completion of the studies, the information collected by the University will be anonymized and might be used for analyses and statistical processing necessary to substantiate the decisions of the institution's management, for a 10-year period, save the personal data necessary for the record of the study documents which are archived, processed and managed on a permanent basis.

In accordance with the provisions of the applicable legislation, you have the following rights: to be informed, to access your own data, to intervene on your personal data, to object, not to be submitted to an individual decision by filing a written application, dated and signed, to Transilvania University of Braşov, to appeal to the court.

The provision of personal data, part of them collected within the admission procedure, is a prerequisite for concluding the Contract of Academic Studies; failure to provide them makes it impossible to proceed with the tuition relationship.

You have the right at any time to withdraw your consent to the personal data processing, save the processing necessary for the record-keeping of the study documents and the excerpts from the official academic records. Withdrawal of consent does not affect the lawfulness of the consent-based processing made prior to its withdrawal; however, depending on the time of your consent withdrawal you will be informed about its

consequences. Moreover, you have hereby acknowledged that you have the right to appeal to the National Supervisory Authority for Personal Data Processing.

B. Declaration

Given the information above, upon accepting this declaration of consent by handwritten signature, I, the undersigned …… identified through the social security number …….. hereby acknowledge to have been informed that my own personal data are to be stored, processed and used under the provisions of the EU Regulations no. 2016/679 and of the legislation specific to higher education, and of the related legislation, as well as agree for these personal data (SSN included), as they were uploaded personally by the undersigned in the IT system related to the admission to Transilvania University of Brașov, respectively by filling them in for the student file, to be processed and used as specified both during the tuition relationship and subsequently, with a view to managing the study documents and graduates' records, according to the activity and duties of Transilvania University of Brașov.

Surname and forename,
Signature,

b) UNITBV staff

Declaration of Consent to Personal Data Processing

A. Information

Transilvania University of Braşov, headquartered in Braşov, 29 Eroilor Avenue, Braşov county, tel. 0268 410525/0268 413000, represented by Rector Prof. Eng. Ioan Vasile ABRUDAN, PhD, is a personal data controller for the stated purpose "record-keeping of employees, HR reports, public communications according to the employment law (for example, financial disclosure statements, public information according to Law no. 544/2001, etc.) and staff reports (including reports on various mobilities/ business travels), as well as vacancy contests.

In accordance with the current provisions of the legislation on the persons' protection in terms of personal data processing and the free movement of such data, including those of the EU Regulation no.2016/679, Transilvania University of Brașov processes *personal data* on legal grounds and under conditions that ensure the security, confidentiality and respect for the data subjects' rights.

Personal Data are any information about an identified or identifiable natural person. This information may include, but is not limited to name, address, social security number, phone number, social condition, image, health condition, and any other kind of necessary information related to the individualization and record-keeping of the employees and vacancy candidates.

Personal data may be communicated between Transilvania University of Braşov and other institutions or public bodies in the field of education, social insurance, health insurance, tax authorities, which may use the information for purposes related to the employees' rights.

Your data are necessary for compiling your personal file within Transilvania University of Brașov (according to the vacancy contest procedures, the data and documents submitted in the contest phase will be taken over and processed in the personal file after signing the labour contract) and they will be processed for the following purposes:

- to fulfil the main scope of activity, respectively education and culture, in the sense of initiating and conducting the legal relationship between you and UNITBV;
- in order to improve the way of communication with the employees/wage earners, via email, for the operative and efficient communication of the information necessary to properly conduct the employment relationship between you and UNITBV.
- in order to archive your data and keep the documents and all the certificates and information that you will provide following the contractual relationship with UNITBV.
- to recruit, select, evaluate the University's employed staff;
- to keep records of the UNITBV employees' personal files and to archive them;
- to record accounting information with a view to making payments to the UNITBV employees.
- to help audit the activities conducted in our institution or in collaboration therewith, and to help in the checks performed by the state control bodies, in full compliance with the applicable legal provisions;
- to conduct other specific activities within the scope of UNITBV and/or activities under the aegis of UNITBV.

At the same time, upon cessation of the employment relationship, regardless of the reason, the information collected by the University will be anonymized and may be used for statistical analysis and processing necessary to substantiate the decisions of the institution's management, for a 50-year period; respectively, it

will be used, just as collected, in reporting to other authorities/ institutions in the field of the employees' social insurance.

In accordance with the provisions of the applicable legislation, you have the following rights: to be informed, to access your own data, to intervene on your personal data, to object, not to be submitted to an individual decision by filing a written application, dated and signed, to Transilvania University of Braşov, to appeal to the court.

The provision of personal data is a prerequisite for concluding and conducting the labour relationship, implicitly for signing the Individual Labour Contract; failure to provide the data, respectively the refusal to have them processed make it impossible to conclude/ conduct the employment relationship, according to art.6 and art.7 in the UE Regulations no.2016/679.

You have the right at any time to withdraw your consent to the personal data processing. The withdrawal of consent does not affect the lawfulness of the consent-based processing made prior to its withdrawal; however, the withdrawal of consent to the processing of your personal data may lead to the unilateral termination of the contractual relationship in force at that time if, for real and objective reasons, it can no longer be conducted as a result of the withdrawal of consent. Moreover, you have hereby acknowledged that you have the right to appeal to the National Supervisory Authority for Personal Data Processing.

B. Declaration

Given the information above, upon accepting this declaration of consent by handwritten signature, the undersigned (surname, forename) ……. identified through the social security number …….. I hereby acknowledge to have been informed that my own personal data are to be stored, processed and used under the Law of Higher Education no. 199/2023, with subsequent amendments; I declare to have been informed about giving consent to personal data processing, to understand and to have been explained in common terms the purpose of the future processing of my personal data, and to herewith agree by signing this information about the processing of my personal data by the UNITBV controller as specified herein.

Signature ……

Application form for Pseudonymization

according to the EU Regulations no. 2016/679, with a view to processing the personal data in the documents displayed on the University's public website, as an obligation imposed according to the institutional transparency procedures.

The undersigned ....., employed at Transilvania University of Brașov, given the personal data in the personal file and having taken note of the University's policy on institutional transparency.

Considering the provisions of the EU Regulations no. 2016/679 on the right to pseudonymization, respectively the removal of the surname, forename and father's initial (or any other personal data that would make it possible to identify the person concerned) on the documents that will be made public (such as institutional reports displayed on the intranet, reports on the University's activity, etc.),

I request the pseudonymization of my personal data as regards the public communication on the University's website, for the purposes of which I understand that I, the undersigned, will be associated with a personal number assigned in this regard.

Date Surname and Forename

APPENDIX 3

Minimum Mandatory Content of the Declaration of Consent to Personal Data Processing

Transilvania University of Braşov, headquartered in Braşov, 29 Eroilor Avenue, Braşov county, as a controller, processes your personal data on the basis of and in strict compliance with the provisions of the Regulations no. 679/2016 on the natural persons' protection in terms of personal data processing.

According to the requirements of the aforementioned Regulations, mere personal data collection involves processing, therefore we have to obtain your prior written consent for these operations. We let you know that, considering the contractual relationship to be concluded between the controller, on the one hand, and you, on the other hand, the refusal to give your consent to personal data processing will entail failure to conclude this contractual relationship pursuant to art. 6 and 7 hereof.

Considering that, failing this personal data processing agreement, the controller cannot conclude any contract with you, the signing of this information implies prior written consent to personal data processing, according to the following.

Your personal data are necessary and will be processed with a view to achieving the following objectives:

A) to fulfill the main scope of activity, namely education and culture, for the purposes of initiating and properly conducting the legal relationship between you and UNITBV;

B) to improve the way of communication with undergraduate/graduate/doctoral students, by email, for the operative and efficient communication of the information necessary to conduct the contractual relationship between you and UNITBV.

C) to archive your data and keep the diplomas, as well as all certificates and accreditations that you will obtain following the conduct of your contractual relationship with UNITBV.

The collected information is intended to be used by the controller and is communicated only to those users within UNITBV who have the obligation to process personal data, but also the correlative obligation to ensure their confidentiality. For any requests regarding the application of these Regulations, withdrawal of consent, access to the personal data, you can send an application in this regard to the General Secretariat of UNITBV, which will forward it to the data protection officer, so that you can receive an answer with no delay.

Pursuant to **art. 7 of the Regulations** no. 679/2016 you have the right to withdraw at any time the consent given by signing this information, just by written request addressed to UNITBV in this regard. We inform you, however, that the withdrawal of consent to the processing of your personal data may lead to the unilateral termination of the contractual relationships that will be in force at that time, if for real and objective reasons they can no longer be continued as a result of the withdrawal of consent.

Pursuant to art. 13 of the same Regulations, you have the right to obtain this information about the data collected by UNITBV, you have the right to access these data, to rectify them and even to restrict their processing. At the same time, you have the right to object to the processing of your personal data and to

request the deletion of these data, save the situations expressly provided for in the law, when data processing by UNITBV is mandatory. For the exercise of these rights, you can send a written, dated and signed request to the General Secretariat of UNITBV, which will forward it to the management and to the data protection officer.

Moreover, you have the right to file a complaint with the National Supervisory Authority for the Processing of Personal Data against the way in which UNITBV conducts personal data collection and processing. Your right to address to a court of law is also acknowledged.

The undersigned _____, residing in _____,

Identified through _____ I hereby declare to have been informed about giving consent to personal data processing, to **understand** and **have been explained,** in common terms, the purpose of the future processing of my personal data, as well as to agree, by signing this information, with the processing of my personal data by the UNITBV controller.

(signature)

APPENDIX 4

Instruction/Minimum Requirements for the Personal Data Collection and Processing in the Procedures of Admission to Academic Studies

Transilvania University of Brașov, through the admission application, will process personal data, such as surname and forename, SSN, telephone, email address, as well as any other data categories that the candidates directly provide in the context of creating the user account at the time of signing up in this admission application.

Transilvania University of Brașov collects data on electronic media, and then the data collected in the stage of pre-registration/registration via the admission application will be managed at the level of the faculty secretariats, respectively of the Interdisciplinary Doctoral School.

Personal data are used as follows:

- record in the University's database;
- to manage the relationship with candidates and provide support, in the interest of supplying adequate and up-to-date information through the website;
- to draw up the documents related to each candidate/student and the study documents.

Through the admission application, Transilvania University of Brașov provides access and at the same time makes known its educational services in order to facilitate the candidates' application during the admission.

Basis: The processing of the candidate/student data for this purpose is based on the agreement and consent to personal data processing, as well as on the Contract of Admission concluded between the student and Transilvania University of Brașov, at the time of pre-registration/registration.

Each candidate's providing data in this regard is voluntary. Refusal to provide consent to candidate data processing for this purpose would make it impossible for the application user to be a candidate for admission, or later to have his/her study documents, as well as other documents related to his/her status as a candidate/student, drawn up.

Each candidate's rights

Under the conditions provided for in the legislation on the personal data processing, the candidates, as data subjects, have the following rights:

- **the right to be informed**, respectively the right to receive details on the processing activities conducted by Transilvania University of Brașov, as described herein;
- **the right of access to data**, respectively the right to obtain the consent of Transilvania University of Brașov to personal data processing, as well as details on the processing activities such as the way in which the data are processed, the purpose for which the processing is done, the data recipients or categories of data recipients, etc;

- **the right to rectification**, respectively the right to obtain the correction, without undue delay, by Transilvania University of Brașov of the inaccurate/unconfirmed personal data, as well as the filling in of the incomplete data; The rectification/completion will be communicated to each recipient to whom the data will have been sent, unless this proves impossible or requires disproportionate effort;
- **the right to data deletion**, without undue delay, ("the right to be forgotten"), if the personal data have been processed illegally (namely, in infringement of GDPR - the UE Regulations no.679/2016 or the data subject's rights), and unless the exercise of this right prejudices the educational activities and obligations of the University as a higher education institution;
- **the right to restrict processing to the extent that** the person contests the accuracy of the data, for a period that allows the controller - the University to check the data accuracy;
- **the right to data portability**, respectively the right to receive the personal data in a structured, commonly used way and in an easy-readable format, as well as the right for Transilvania University of Brașov to transmit these data to another data controller, to the extent that the conditions stipulated by the law are met;
- **the right to opposition** – the data subject's right to oppose any processing, including the creation of profiles.

Transilvania University of Brașov makes available a set of standard application forms for exercising these rights. You can also express your views on data portability by emailing to the address **dep-protectiadatelor@UNITBV.ro.**