

## PRIVACY POLICY

### 1. Purpose

Given the concern of the University of Bucharest ("**University**") for compliance with the law in general and with the rules designed to protect personal data and privacy of individuals in particular, it is necessary to adopt this policy ("**Policy**") governing the processing of personal data carried out by or on behalf of the University.

The purpose of the Policy is to describe the rules and procedures applicable to personal data processing operations carried out by/on behalf of the University, so that the University complies with the following general rules on the protection of personal data throughout its activities (but not limited to):

- (i) the processing operations comply with the University's standards, the legislation in the field of personal data processing in Romania and the European Union and the most advanced best practices and standards in the field;
- (ii) the rights of the data subjects to whom the data relating to the data processed by the University relate are fully respected and that those data subjects are protected against the risks arising from the processing of their personal data by the University;
- (iii) The University to adopt a transparent, consistent and predictable position on how it processes personal data, which gives confidence to students, staff, employees and all other data subjects.

#### 1.1. Legal framework

As of 25 May 2018, the main piece of legislation applicable throughout the European Union is Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC, also known as the *General Data Protection Regulation* ("GDPR" or the "Regulation"). The GDPR creates a single EU legal regime applicable to the processing of personal data and is directly applicable in Romania. All persons within the Companies will be obliged to comply with the GDPR and to pay due attention to the rights that individuals have in relation to their personal data.

### 2. SCOPE OF THE POLICY

## 2.1. Personal scope

The policy is applicable to the following persons, who are bound by its provisions:

- 2.1.1. all directorates/faculties of the University;
- 2.1.2. all Employees;
- 2.1.3. all Employees.

## 2.2. Material scope

The policy applies to all personal data processing operations carried out by/on behalf of the University.

## 2.3. Temporal scope

- 2.3.1. The policy applies to personal data processing operations carried out on behalf of the University on or after 25 May 2018 (inclusive), regardless of whether those processing operations are ongoing on that date or begin on or after that date.
- 2.3.2. Employees and Collaborators will be made aware of its provisions and the most important Employees and Collaborators in terms of the data processing activities they are involved in have been and will be trained on its provisions and on the Romanian and European Union legislation on personal data protection.

## 3. Responsibilities

### 3.1. University Management

Management has the following responsibilities:

- 3.1.1. approves the general policy, subsequent policies and objectives on the protection of personal data,
- 3.1.2. ensure that the necessary resources are available to implement technical and organisational measures to protect data and respect the rights of data subjects,
- 3.1.3. designate a Data Protection Officer (if required by law) and ensure that he/she has the necessary competences,

- 3.1.4. ensure that the Data Protection Officer is adequately and timely involved in all aspects of personal data protection,
- 3.1.5. ensure that the Data Protection Officer does not receive any instructions with regard to the performance of the assigned tasks,
- 3.1.6. communicates the importance of compliance with the requirements of EU Regulation 679 /2016 - GDPR. Data Protection Officer

**The Data Protection Officer** reports directly to the University Management.

The Data Protection Officer has at least the following responsibilities:

- 3.1.7. informs and advises University staff and persons authorised by the University to process personal data operating under the GDPR and other national or EU data protection provisions,
- 3.1.8. coordinates the identification and evaluation of data processing activities carried out in the University,
- 3.1.9. participates in meetings with the management of directorates, services, departments, faculties and other organisational units within the University when new processing operations are conceived, to ensure that the principle of data protection is respected from the moment of conception at all levels,
- 3.1.10. maintain records of processing activities in accordance with Article 30 of the GDPR,
- 3.1.11. monitor compliance with the GDPR, other national or European Union data protection provisions and the University's policies and procedures regarding the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations and related audits,
- 3.1.12. provide advice when requested on the Data Protection Impact Assessment (DPIA) and monitor its performance in accordance with Article 35,
- 3.1.13. cooperate with the supervisory authority,
- 3.1.14. draws up and updates internal data protection policies and procedures,

- 3.1.15. conducts audits to determine compliance with internal data protection policies and procedures and needs for improvement,
- 3.1.16. implements a training programme on personal data protection for University staff involved in processing activities,
- 3.1.17. monitors changes to legislation and makes recommendations to ensure compliance with these changes,
- 3.1.18. maintain a record of privacy breaches in processing operations carried out by the University,
- 3.1.19. provides advice on how to deal with breaches of privacy,
- 3.1.20. ensure that the University responds to requests from data subjects within the legal deadlines,
- 3.1.21. act as a contact point with EU residents, the national supervisory authority and the authorities of the other EU countries and internal teams on processing-related issues, including prior consultation as referred to in Article 36, and consult the national supervisory authority, where appropriate, on any other matter,
- 3.1.22. has an obligation of secrecy or confidentiality in the performance of its duties.

In carrying out his/her duties, the Data Protection Officer ("DPO") shall consider the risks associated with the processing operations, taking into account the nature, scope, context and purposes of the processing.

### 3.2. **Management Faculties / Heads of organisational entities**

Faculty Management / Heads of Organizational Entities are responsible for:

- 3.2.1. day-to-day implementation of the requirements for the secure management of personal data,
- 3.2.2. ensuring that the established technical, physical and organisational security measures are properly implemented and applied by all staff,
- 3.2.3. providing the resources and conducting the necessary analysis to ensure that information and information assets are adequately protected in their area of responsibility,

- 3.2.4. informing the Data Protection Officer of actual or suspected breaches of data privacy policies in their area of responsibility (data privacy incidents).

### 3.3. **Staff involved in processing**

Processing staff have the following responsibilities:

- 3.3.1. comply with all applicable privacy and data protection policies for their jobs,
- 3.3.2. are responsible for maintaining the protection and confidentiality of all information entrusted to them,
- 3.3.3. informs Faculty Management/Heads of organisational entities of actual or suspected breaches of data privacy policies in their area of responsibility (data privacy incidents).

### 3.4. **Staff not directly involved in processing**

Staff not directly involved in processing have the following responsibilities:

- 3.4.1. comply with all applicable privacy and data protection policies for their jobs,
- 3.4.2. informs Faculty Management/Heads of organisational entities of actual or suspected breaches of data privacy policies in their area of responsibility (data privacy incidents).

### 3.5. **Contributors**

Employees involved in processing have the following responsibilities:

- 3.5.1. complies with all applicable privacy and data protection policies for personal data processing carried out,
- 3.5.2. are responsible for maintaining the protection and confidentiality of all information entrusted to them,
- 3.5.3. informs Heads of organisational entities of actual or suspected breaches of data privacy policies in their area of responsibility (data privacy incidents).

### 3.6. **Authorised persons**

Authorised persons involved in processing have the following responsibilities:

- 3.6.1. complies with all applicable privacy and data protection policies for personal data processing carried out,
- 3.6.2. are responsible for maintaining the protection and confidentiality of all information entrusted to them,
- 3.6.3. informs Heads of organisational entities of actual or suspected breaches of data privacy policies in their area of responsibility (data privacy incidents).

### 3.7. **General responsibilities**

Within the University, every Employee and Collaborator has a general obligation to ensure that personal data processing operations in which he/she is involved in carrying out work on behalf of or in the interests of the University are carried out lawfully and in accordance with the Policy. In the event of any doubt as to the lawfulness and/or compliance with the Policy of a particular action, any Employee or Contributor has an obligation to suspend that action, contact the DPO and only resume that action at a later date and only to the extent that the lawfulness and compliance with the Policy has been confirmed by the DPO.

## 4. **Principles**

4.1. According to Article 5 of the Regulation, the principles relating to the processing of personal data have been defined as follows:

- 4.1.1. **Lawfulness, fairness and transparency:** personal data will be processed lawfully, fairly and transparently by the University towards the data subject; the provisions of the personal data protection legislation must always be respected, including the obligation that any processing of personal data must be attributed a basis and the obligation to provide information to the data subject about how his/her personal data will be processed.
- 4.1.2. **Purpose limitations:** personal data will be collected by the University for specified, explicit and legitimate purposes;
- 4.1.3. **Data minimisation:** personal data will be adequate, relevant and limited to what is strictly necessary in relation to the purpose(s) for which it is processed by the University;
- 4.1.4. **Accuracy:** personal data will be accurate and, where necessary, kept up to date. The University will take all necessary steps to ensure

that data which are inaccurate (in relation to the purposes of the processing) are erased or rectified without delay;

- 4.1.5. **Storage limitations:** personal data shall be kept by the University in a form which permits identification of data subjects for no longer than is necessary for the purposes of the processing; data shall be erased or made anonymous when the purposes of the processing have been fulfilled;
- 4.1.6. **Integrity and confidentiality:** personal data will be processed by the University in a way that ensures their adequate security. The University has taken and maintains appropriate technical or organisational measures to ensure that data is protected against unauthorised/ unlawful processing and accidental loss/ destruction/ damage;
- 4.1.7. **Accountability:** the University, as the controller of personal data, is responsible for compliance with the above principles and must at all times be able to demonstrate that those principles are respected;

In addition to complying with the above principles, the University will keep a record of its data processing activities, personal information shared and security measures implemented.

In the event of a data protection breach under the Regulation, the security incident will be reported to the national supervisory authority within 72 hours of discovery of the breach.

If requests are received from data subjects regarding the processing of personal data, the response must be sent no later than 30 days after receipt of the request, in certain cases the deadline may be extended by up to 30 days.

Compliance with GDPR is the responsibility of all members of the University. Any deliberate breach of this policy may lead to disciplinary action, withdrawal of access to University facilities or even prosecution.

## 5. **Receipt of documents containing personal data**

Documents will be kept in written and/or electronic format and will be stored in secure locations with an appropriate level of security and with access permitted only to authorised personnel.

All users of personal data must ensure that data is not disclosed to any unauthorised third party in any form, whether accidentally or otherwise

mod. Electronic data security must be ensured in accordance with the IT Information Security Policy and related procedures.

Regardless of their type, Documents shall never be left unattended in a place accessible to the public. During the period in which they are required for consultation or amendment, documents will be kept in such a way that unauthorised persons cannot view/access them.

During periods when access to them is not strictly necessary and relevant, Documents will be stored in secure lockers which, as far as possible, will be monitored by video surveillance.

Documents shall be stored in an organised manner that allows their subject matter to be identified without the need to actually access the information contained therein.

When not required for consultation or amendment, and in any event no later than each day at the end of the programme, each person holding Documents shall ensure that Documents, either originals or copies, are stored in lockers/lockable filing cabinets. The University may conduct audit activities to verify compliance with this obligation.

## **6. Lawfulness of processing**

### **6.1. Data storage**

The personal data collected is stored in premises and on equipment located within the University of Bucharest, on servers belonging to the University installed in the Telekom datacenter or using the storage services of the G-Suite platform for educational institutions. For limited periods of time, data can also be stored locally by University employees, in electronic documents stored on different equipment or on paper documents.

Each organisational entity within the University of Bucharest is responsible for ensuring appropriate retention periods for the information it holds and manages, based on the organisation's archival nomenclature. Storage periods will be established based on legal and regulatory requirements, industry guidelines and best practices.

**Personal data must be kept only for the period of time necessary to carry out the processing for which they were collected.**

Details on the safe disposal of paper records or electronic records can be found in the Records Disposal Procedure.

### **6.2. Grounds for personal data processing activities**



In order for the University to lawfully process personal data, at least one of the following conditions must be met:

- 6.2.1. the valid consent of the data subject has been collected in advance;
- 6.2.2. processing is necessary for the performance of the subject matter of a contract;
- 6.2.3. the processing is necessary for the fulfilment of a legal obligation of the University;
- 6.2.4. processing is necessary to protect the vital interests of the data subject;
- 6.2.5. 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 University;
- 6.2.6. the processing is necessary to protect the legitimate interests of the University or of a third party and does not interfere with the rights and freedoms of the data subject (this condition may not be used by public authorities in the performance of their public tasks).

The processing of "special categories" of personal data requires additional, stricter conditions to be met under Article 9 of the GDPR. Article 9 prohibits the 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 unique identification of a natural person, data concerning health or data concerning the sex life or sexual orientation of a natural person, except in the following cases:

- 6.2.7. The data subject has explicitly consented to the processing of these personal data for one or more specific purposes;
- 6.2.8. The processing is necessary for the purposes of fulfilling obligations and exercising specific rights of the University or the data subject in the field of employment and social security and social protection;
- 6.2.9. The 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;
- 6.2.10. The processing is carried out within the framework of their legitimate activities and with appropriate safeguards by a foundation, an association or any other non-profit-making body of a political, philosophical, religious or trade-union nature, provided that the processing relates solely to members or former members of that body or to persons with whom it has contact.

permanent in relation to its purposes and that personal data are not disclosed to third parties without the consent of the data subjects;

- 6.2.11. The processing relates to personal data which are manifestly made public by the data subject;
- 6.2.12. The processing is necessary for the establishment, exercise or defence of a right in court or whenever the courts act in the exercise of their judicial function;
- 6.2.13. The processing is necessary for reasons of substantial public interest;
- 6.2.14. The processing is necessary for the purposes of preventive or occupational medicine, the assessment of the employee's ability to work, the establishment of a medical diagnosis, the provision of health or social care or medical treatment or the management of health or social care systems and services;
- 6.2.15. The processing is necessary for reasons of public interest in the field of public health, such as protection against serious cross-border threats to health or ensuring high standards of quality and safety of healthcare and medicinal products or medical devices, under Union or national law providing for appropriate and specific measures to protect the rights and freedoms of the data subject, in particular professional secrecy; or
- 6.2.16. The processing is necessary for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes.

### 6.3. **Consent of data subjects as a basis for processing**

Consent of the data subject may be one of the legal grounds for processing personal data and the University must ensure that the consent of the data subject is validly collected whenever the processing activity to be carried out is based on consent. Any person who has given consent has the right to withdraw consent at any time.

Consent is defined as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or other clear affirmative action, signifies his or her agreement to the processing of personal data relating to him or her". GDPR provides that no response, pre-ticked boxes or inactivity does not constitute valid consent (opt-out consent)

In the case of employees, consent may not be used as a basis for processing personal data, as this is caused by the obvious imbalance in the relationship between the University and the data subject (employee), and in such cases, it cannot be

considered freely given consent. The University will therefore need to identify alternative grounds for such processing.

Further information on obtaining consent can be found in the Procedure for Giving and Withdrawing Consent.

#### 6.4. **Legitimate interest as a basis for processing**

Legitimate interests of the University, including those of an organisation to which personal data may be disclosed or of a third party, may constitute a legal basis for processing, provided that the interests or fundamental rights and freedoms of the data subject are not overridden, taking into account the reasonable expectations of data subjects based on their relationship with the controller.

The following are examples of personal data processing activities based on legitimate interest

- 6.4.1. for organisational purposes
- 6.4.2. when using employee data to promote the University on its websites
- 6.4.3. when using student data for the submission of questionnaires to evaluate activities carried out within the University;
- 6.4.4. Processing strictly necessary to prevent fraud or to protect certain assets;
- 6.4.5. to ensure the security of computer networks and information.

The carrying out of personal data processing on the basis of legitimate interest must be confirmed by the carrying out of a Legitimate Interest Assessment carried out in cooperation with the DPO.

Further information on how to assess legitimate interest can be found in the Procedure for assessing legitimate interest.

#### 6.5. **Notions of privacy by design & privacy by default**

Taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of the processing, as well as the risks of varying degrees of likelihood and severity to the rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of establishing the means of processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to effectively implement data protection principles, such as data minimisation, and to incorporate the necessary safeguards in the processing, in order to

meet the requirements of this Regulation and protect the rights of data subjects.

Under the GDPR, the University is required to consider the impact on data privacy during all processing activities. This includes implementing appropriate technical and organisational measures to minimise the risk to personal data.

It is particularly important to consider privacy issues when new processing activities arise or new procedures or systems involving personal data are put in place. The GDPR imposes a specific requirement on privacy by design, emphasising the need to implement appropriate technical and organisational measures during the design stages of a process and throughout the lifecycle of the relevant data processing to ensure that data protection is properly managed.

According to Decision No 174 of 18.10.2018 on operations for which it is mandatory to carry out a personal data protection impact assessment (DPIA), the following require a data protection impact assessment (DPIA): processing of large amounts of personal data, automated profiling, processing of special categories of personal data or monitoring of publicly assessable areas (video surveillance).

Information on when and how to conduct a DPIA can be found in the Data Protection Impact Assessment Procedure.

#### **6.6. Information to data subjects**

In line with the requirements of the "fairness and transparency" principle on data protection, the University is obliged to provide data subjects with a "privacy notice" to let them know how it uses their personal data.

Privacy notices are posted at access points in the organisation, on the unibuc.ro website and at other points deemed relevant in terms of access by data subjects. Any processing of personal data beyond the scope of the standard notice will need to be provided separately.

Further information on the privacy notice can be found in the Procedure for informing data subjects.

#### **6.7. Mapping and inventory of data processing activities**

As data controller, the University is obliged to keep a record of the personal data processing activities carried out. Among other things, this record must contain details of how personal data are processed, the types of individuals about whom information is held, indications of

third party organisations with whom personal data is shared and if personal information is transferred to countries outside the EU. The University carries out processing activities on the following categories of individuals:

- Students, Master's students, PhD students (prospective, current and alumni);
- Employees (potential, current and former);
- Data subjects other than candidates, employees and former employees

Staff engaged in new activities involving the processing of personal data and who are not covered by one of the existing records of processing activities should inform the Data Protection Officer ([dpo@unibuc.ro](mailto:dpo@unibuc.ro)) before starting the new activity.

Further information on the Logging of processing activities can be found in the Procedure for the Logging of Personal Data Processing.

## 6.8. **Informing employees about the provisions of the Regulation**

According to the GDPR requirements, the University is obliged to train all employees with responsibilities involving the processing of personal data or who have permanent/regulated access to such data on the GDPR requirements as well as on how to implement these requirements within the University of Bucharest.

To this end, the Data Protection Officer is designated to implement the training programme on personal data protection for University staff.

More information on the training programme can be found in the GDPR Training Procedure.

## 6.9. **Rights of data subjects**

### 6.9.1. Right of access

The data subject has the right to obtain from the University confirmation as to whether or not personal data relating to him or her are being processed. If the University processes his or her personal data, the data subject has the right of access to that data and to the following information:

- the purposes of processing;
- the categories of personal data concerned;
- the recipients/categories of recipients to whom data have been or will be disclosed, in particular

- recipients from third countries or international organisations;
- the period for which the data is intended to be stored or, if this is not possible, the criteria used
- to determine the storage period;
- the fact that the data subject has the right to request the University to rectify, erase or delete data
- restriction of data processing and the right to object to processing;
- the right of the data subject to lodge a complaint with the supervisory authority for processing
- personal data;
- if the data are not collected from the data subject, any information on the source;
- the existence of an automated decision-making process (including profiling) and information on the logic used and the significance and expected consequences of the processing for the data subject.

The data subject must be able to exercise this right easily and at reasonable intervals.

If the data subject's request is in electronic format and he or she does not request a response in another format, the University's response will be sent in a commonly used electronic format.

#### 6.9.2. Right to rectification

If his/her personal data are inaccurate or incomplete, the data subject has the right to have them rectified by the University (as controller) without undue delay.

Depending on the purpose of the processing of personal data, the data subject has the right to have his/her data processed by the University completed (if applicable), including following the provision of additional statements by the data subject.

#### 6.9.3. Right to erasure of data ("right to be forgotten")

The data subject shall have the right to request that his or her personal data are erased without undue delay if it is no longer necessary for them to be processed by the University (as controller of personal data).

The data subject has the right to erasure of data relating to him or her in the following situations:

- its personal data are no longer necessary for the purposes for which the University collected (processed) them;
- the data subject has withdrawn the consent on the basis of which the processing took place and there is no other basis on which the University can process his/her data;
- the data subject objects to the processing (on the basis of his/her right to object) and there are no legitimate grounds for the University to process the data further;
- The university processed the data illegally;
- there is a legal obligation of the University to delete data;
- the data collection took place in connection with the provision of information society services to a minor.

The data subject has the right to erasure of data that the University processes even if the processing has not caused him or her any damage or inconvenience.

The University may refuse to comply with a request to delete personal data if the processing is necessary:

- for the exercise of the right to free expression and information;
- to comply with a legal obligation to process, to fulfil a task carried out in public interest or in the exercise of an official authority vested in the University;
- for reasons of public interest in the field of public health;
- for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes in accordance with the GDPR, insofar as the right to erasure of the data is likely to render impossible or seriously affect the achievement of the purposes of the processing concerned;
- to establish, exercise or defend a right in court.

In the (unlikely) event that the University has made public the personal data of the data subject concerned and has to comply with the data subject's request for erasure, it will take reasonably available measures to inform

controllers processing those data that the data subject has requested that they delete links to or, where applicable, reproductions of those data.

#### 6.9.4. Right to restrict processing

The University will comply with a request to restrict data processing if at least one of the following conditions is met:

- the data subject disputes the accuracy of the data that the University is processing - in this case, the University will stop processing until it has verified the accuracy of that data;
- the processing is unlawful - in which case the data subject, although entitled to have his or her data erased (see section on the Right to erasure of data ("right to be forgotten")), objects to the erasure and instead asks the University to restrict its use;
- The University no longer needs the personal data, but the data subject requests the data concerned for the purpose of establishing, exercising or defending a legal claim;
- the data subject has objected to processing necessary for the performance of a task carried out in the public interest or resulting from the exercise of official authority vested in the University (as controller) or the data subject has objected to processing necessary for the purposes of legitimate interests of the University (as controller) or of a third party - in all these cases, the University will stop processing the data subject's data during the period in which it verifies whether the legitimate grounds on which the data are processed by the University outweigh the data subject's rights.

In such cases, the University, as controller, has the right to store the data in question, but will not process it further. In turn, the storage of the data must only take place to the extent necessary for the University to ensure that the restriction of the processing of that data will be respected in the future, *i.e.* if the data subject exercises the right to restrict the processing, the University's activities in processing that data will be blocked.

However, the University may continue to process (and other than by storage) data whose processing has been restricted by the **data subject if and to the extent that:**

- the data subject consents to the processing;
- processing is necessary for the establishment, exercise or defence of legal claims;



- the processing is necessary for the protection of the rights of another natural or legal person;
- processing is necessary for reasons of substantial public interest of the European Union or of a Member State of the European Union.

Before lifting the restriction on processing, the data subject will be informed.

By way of example, depending on the specific way in which it processes the data concerned, in order to comply with the request to restrict processing, the University may temporarily move the data whose processing is restricted to another processing system, block users' access to that data or adopt any measures having a similar effect.

It shall also be clearly indicated in the system and in the record of processing operations kept by the University that the processing of the data concerned has been restricted, in order to ensure that the data concerned will not be processed (including by altering them) after the restriction. In this regard, the persons responsible for processing the data concerned and the DPO will be informed.

#### 6.9.5. Right to data portability

Data subjects may obtain from the University the personal data that the University processes, to use them for the purposes they wish and to be able to transfer them from one medium to another in a secure and easy way

The data subject has the right to portability only in relation to data which the University processes on the basis of his or her consent, for the performance of a contract to which the data subject is a party or for taking steps prior to the conclusion of a contract, at the request of the data subject.

#### 6.9.6. The right to oppose

Data subjects have the right to object to the processing of their personal data which is necessary for the performance of a task carried out in the public interest, results from the exercise of official authority vested in the University or is necessary for the legitimate interests of the University or of a third party.

Data subjects also have the right to object to processing for direct marketing purposes.

The rights set out above will be made expressly, clearly and separately from other information known to the data subjects at the latest at the time of the University's first communication with them.

Data subjects also have the right to object to processing for the purposes of

scientific or historical research or for statistical purposes, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

The right not to be subject to a decision based solely on automated processing (including profiling).

In the case of automatic processing of personal data that the University carries out, data subjects have the right not to be subject to decisions based on such processing which produce legal effects concerning them or otherwise significantly affect them.

However, data subjects will not benefit from the above right when the decision (i) is necessary for the conclusion or performance of a contract between them and the University, (ii) is required by law under the GDPR, or (iii) is based on the explicit consent of the data subject.

Where the decision is necessary for the conclusion or performance of a contract between the data subject and the University or is based on the explicit consent of the data subject, the data subject shall have the following rights: (i) the right to obtain human intervention in the taking of the decision, (ii) the right to express his or her point of view and (iii) the right to appeal the decision.

Decisions based on automatic processing, where permitted, will not be based on special categories of personal data unless the data subject has expressly consented or the processing of those data is necessary for reasons of substantial public interest under the law.

























The Regulation gives data subjects the right to access personal information held by the University. The purpose of an access request is to allow data subjects to confirm the accuracy of personal data and to verify the lawfulness of the processing in order to enable them, if necessary, to exercise their rights of correction or objection.

The University must respond to all requests for access to information, and information will normally be provided free of charge.

Any requests made to invoke any of the above rights must be dealt with promptly and in any event within 30 days of receipt of the request. In certain cases, the time limit may be extended by up to 30 days.

Staff should consult the Data Protection Officer if such requests are received. The following table summarises how the rights can be exercised.

<b>Basis of processing</b>
----------------------------

<b>Rights of the data subject</b>	<b>Consent</b>	<b>Contract execution</b>	<b>Legal obligation</b>	<b>Legitimate interest</b>
<b>Withdrawal</b>				
<b>Access</b>				
<b>Correction</b>				
<b>Delete</b>				
<b>Restriction</b>				
<b>Portability</b>				

More information and guidance on the handling of subject access requests can be found in the Subject Access Request Procedure.

#### 6.10. **Authorised persons**

Where a processing of personal data is to be carried out on behalf of the University, the University shall only use processors providing sufficient guarantees for the implementation of appropriate technical and organisational measures so that the processing complies with the requirements laid down in this Regulation and ensures the protection of the rights of the data subject.

The processing carried out by a processor must be governed by a contract or other legal act which is binding on the University's processor and which must set out at least the object and duration of the processing, the nature and purpose of the processing, the type of personal data, the categories of data subjects and the measures to be implemented by the processor.

Where a processing of personal data is to be carried out in a joint venture between two or more controllers, an agreement, contract or other legal act must be concluded specifying the responsibilities of each party with regard to the fulfilment of their obligations under the GDPR Regulation, in particular on how to exercise the rights of data subjects and the duties of each party to provide information to data subjects of the processing.

Irrespective of the terms of the agreement, contract or legal act referred to in the previous paragraph, the data subject may exercise his or her rights under the GDPR in respect of and in relation to each of the controllers.

Staff must consult with the Data Protection Officer if they conclude

a new contract involving the sharing or processing of personal data.

Further information on managing relationships with other organisations can be found in the Procedure for the Management of Authorised Persons.

#### 6.11. **Data transfer**

Certain conditions must be met before personal data can be shared by the University with a third party.

As a general rule, personal data should not be transmitted to third parties, especially if they involve special categories of personal data, but there are certain circumstances when transmission is permitted.

Any transfer of personal data must comply with the principles of data processing, i.e. be lawful and fair to the data subjects and meet one of the processing conditions. Legitimate reasons for the data transfer would include:

- fulfilment of a legal obligation;
- where the data subject has been informed about the transfer of his or her data and has explicitly consented to the transfer.

The University will ensure that the third party will comply with all GDPR requirements, in particular with regard to keeping information secure.

#### 6.12. **Compliance with the provisions of Law 544/2001 on free access to information of public interest**

According to Law 544/2001, art.12, information on personal data is exempted from the free access of citizens. It is also stated in Art. 14 that information on the citizen's personal data may become information of public interest only to the extent that it affects the capacity to exercise a public function.

Staff receiving requests for information under Law 544/2001 must also check that the data confidentiality requirements are met.

#### 6.13. **Transfers of personal data outside the EU**

The transfer of personal data to a third country or an international organisation may take place when the European Commission has decided that the third country, a territory or one or more specified sectors in that third country or international organisation ensures an adequate level of protection. Transfers made under these conditions do not require special authorisations.

At the date of approval of this document, the countries considered by the European Commission as providing an adequate level of protection are: Andorra, Argentina, Canada (trade organisations only), Faroe Islands, Guernsey, Jersey and Man, Israel, New Zealand, Switzerland and Uruguay.

In the absence of a decision, the University may transfer personal data to a third country or international organisation only if the controller or processor has provided adequate safeguards and provided there are enforceable rights and effective remedies for data subjects.

For certain specific situations, the GDPR provides for exemptions from the prohibition on transfers of personal data outside the EU. These exemptions include:

- 6.13.1. the data subject has explicitly agreed to the proposed transfer;
- 6.13.2. the transfer is necessary for the performance of a contract between the data subject and the controller or for the application of pre-contractual measures adopted at the request of the data subject;
- 6.13.3. the transfer is necessary for the conclusion of a contract or the performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
- 6.13.4. the transfer is necessary for important reasons of public interest;
- 6.13.5. the transfer is necessary for the establishment, exercise or defence of legal claims;
- 6.13.6. the transfer is necessary for the protection of the vital interests of the data subject or of other persons where the data subject lacks the physical or legal capacity to give his or her consent;

#### 6.14. **Conducting data processing activities for research purposes**

Personal data used for research purposes by University of Bucharest staff must be treated in accordance with the GDPR and its data protection principles. In addition to meeting the GDPR requirements, research involving personal data must comply with the ethical procedures established at the University. To meet the transparency requirement, researchers must provide privacy notice to the participants in the research project, both when data are collected directly from the data subject and when the researcher uses personal data obtained through a third party. It is important that staff collecting data for research or consultancy purposes include an appropriate form of consent in any

data collection.

#### 6.15. **Processing of personal data through video means**

The University employs a 24/7 video surveillance system to prevent, deter, manage and investigate safety and security incidents, as well as to protect people and property from fire, theft, destruction, attack or any threat. The video surveillance system helps to prevent, deter, manage and, if necessary, investigate safety and security incidents, potential threats or unauthorised physical access, including unauthorised access to secure buildings and protected rooms, IT infrastructure or existing research equipment. The system is not used to monitor employee attendance.

The use of the video surveillance system is mentioned on the pictograms positioned at a reasonable distance from the places where the video surveillance equipment is located, in the premises of the University of Bucharest, as provided for by the GDPR, by Law no. 333/2003 on the security of objectives, goods, values and protection of persons and by Government Decision no. 301/2012 for the approval of the Methodological Rules for the application of Law no. 333/2003 on the security of objectives, goods, values and protection of persons.

The video surveillance operation is coordinated by the Real Estate Directorate through the Security Service. In addition to video surveillance systems installed in accordance with the requirements of Law 333/2003, video surveillance systems are installed in certain areas based on the legitimate interest pursued by the University. The use of these surveillance systems is indicated on pictograms positioned at a reasonable distance from the places where the video surveillance equipment is located.

Further information on video surveillance can be found in the Video Surveillance Procedure

#### 6.16. **Direct marketing activities**

Direct marketing refers to communication (regardless of media) through advertising or marketing materials directed at individuals. Individuals must be able to opt out of lists or databases used for direct marketing purposes. The University must cease direct marketing activity if an individual requests to stop communications.

Direct marketing must also comply with legislation on the processing of personal data and the protection of privacy in the electronic communications sector, which covers marketing by telephone, written communication and e-mail.

**Any direct marketing activities will be based on the data subject's consent.**

### 6.17. **Organisation of events**

The identity of guests attending an event, their images, educational or professional details are personal data as they represent information about identifiable individuals and therefore must be processed in accordance with GDPR principles.

in the case of guests whose personal data are used for the promotion or further presentation of the event via press, posters or websites, explicit consent must be obtained. This is the easiest and safest way to prove that personal data are used in a fair way and in accordance with the rights of the individual. There may also be cases where there is a contract between the University and the guest providing for the use of personal data for the promotion or presentation of the event.

All participants taking part in the event must be informed that photographs or video recordings will be taken. This should be done at the time of the event and, if possible, through the event's promotional page. If there are areas where no photography or video recording is to be taken, these should be highlighted so that they can be used by those participants who do not wish to be photographed or filmed.

Further information on this subject can be found in the Event Organisation Procedure

### 6.18. **Data processing by students**

The University is responsible for personal data processed by students when they process data in accordance with University or legal requirements. These include processing carried out by students appointed to participate in accommodation, camp or scholarship committees.

In these cases, we ensure that the persons processing personal data have been informed of the GDPR requirements and have signed confidentiality undertakings.

Further information on this topic can be found in the Procedure for the use of contributors.

### 6.19. **Online presence**

All websites belonging to the University must comply with the rules established at University level in terms of appearance, security and personal data protection. To comply with GDPR requirements, websites will apply at least the following technical measures:

- posting a cookie management solution and information about the cookies used by the website and how the user can object to their installation;
- posting a privacy notice including the name of the University, the purpose of the processing, the data processed, possible international transfers, the data subject's rights, etc;
- if you want to use the contact data for other purposes (marketing communications, newsletters, etc.) include an information and a form for taking the user's consent and withdrawing it;
- ensuring technical measures for the protection of personal data submitted by the user.

## 6.20. Security incidents

The University is responsible for ensuring appropriate and proportionate security of the personal data it holds. This includes protecting data against unauthorised or unlawful processing and against accidental loss, destruction or damage to data. The University makes every effort to avoid personal data breaches, however, mistakes may occasionally occur. Examples of personal data breaches include:

- 6.20.1. Loss or theft of data or equipment containing personal data;
- 6.20.2. Controls by access improper which to allow unauthorised use;
- 6.20.3. Equipment problems allowing unauthorised access;
- 6.20.4. Unauthorised disclosure (e.g. emails sent to the wrong recipient);
- 6.20.5. Human error;
- 6.20.6. Hacking.

If a data protection breach is observed, it should be reported immediately. Details on how to report a breach and the information that will be requested are included in the Personal Data Breach Management Procedure.

In certain cases of data protection breaches, the University is obliged to report this as soon as possible to the National Data Protection Supervisory Authority.



Personal Data Processing Authority (ANSPDCP), but no later than 72 hours after its discovery.

Details on how to report a breach to the ANSPDCP are included in the Data Breach Notification Procedure.

#### 6.21. **Extent of the incident and responsibilities**

All University employees are obliged to comply with this data protection policy, its guidelines and the requirements specified in the GDPR. Any member of staff who has unauthorisedly disclosed personal information or breached the terms of this Policy may be subject to disciplinary action.

The University could be sanctioned for non-compliance with GDPR. Fines are differentiated according to the breach of the obligations of the University, the processor and so on or the breach of the basic principles for processing, including the conditions for consent, the rights of data subjects and so on.

#### 6.22. **Data Protection Officer**

The University is obliged to appoint a Data Protection Officer (DPO). The Data Protection Officer may be an employee of the University, performing his/her duties under an individual employment contract or may be an external collaborator, performing his/her duties under a service contract. Details in the Procedure for the appointment of the Data Protection Officer.

The Data Protection Officer appointed by the University is **SCA Zorin Vasile Dăscălescu and Associates**.

The role of the Data Protection Officer is to independently ensure the correct application of data protection rules within the University. In doing so, he/she contributes to the protection of the rights and freedoms of individuals whose personal data are processed by the University. to this end, the Data Protection Officer:

- increases awareness of data protection obligations;
- advises staff on data protection; reports non-compliance with applicable rules.

In addition to the general advisory role of the Data Protection Officer, the Data Protection Officer may conduct investigations, on a voluntary basis or upon request, on data protection issues.

You can contact the Data Protection Officer for advice or for requests to investigate a specific issue, for access to personal data or for any matter directly related to his or her duties at the e-mail address: **[dpo@unibuc.ro](mailto:dpo@unibuc.ro)**.