
	<b>Regulation</b> <b>on the processing of information containing</b> <b>personal data in the university management</b> <b>information system "dean's office" (student</b> <b>records)</b>	<b>Code: REG-0-</b> <b>PIDCPSIMUD</b>
		<b>1st edition</b>
		<b>Revision 0</b>

**APPROVED AT TUM SENATE**  
**MEETING**  
**FROM 25.10.2016, REPORT NO.2**

# **REGULATION** **ON THE PROCESSING OF INFORMATION** **CONTAINING PERSONAL DATA** **IN THE RECORD SYSTEM** **"DEAN'S OFFICE"** **(STUDENT RECORDS)**

	<b>Regulation on the processing of information containing personal data in the university management information system "dean's office" (student records)</b>	<b>Code: REG-0- PIDCPSIMUD</b>
		<b>1st edition</b>
		<b>Revision 0</b>

## I. GENERAL PROVISIONS

**1.1.** The Regulation on the processing of information containing personal data in the university management information system "**Dean's Office**" (hereinafter the Regulation) is developed in order to implement within the Technical University of Moldova the provisions of the Law no.133 of July 8, 2011 "On the protection of personal data", and the *"Requirements for ensuring the security of personal data when processing them within the information systems of personal data"*, approved by Government Decision no.1123 of December 14, 2010.

**1.2.** This Regulation regulates the general conditions and requirements for the processing of personal data of TUM students within the University Management Information System "Dean's Office" (hereinafter - SIMU "Dean's Office").

## II. THE OBJECTIVE

**2.1.** Purpose of processing information containing personal data in EMIS


The "Dean's Office", consists in ensuring the registration of information related to the matriculation, expulsion, promotion, success, student mobility.

**2.2.** The following categories of personal data are processed within SIMU "Dean's Office":

- first name, last name;
- sex;
- date and place of birth;
- citizenship;
- IDNP;
- picture;
- military situation;
- personal data of family members;
- bank details for the transfer of scholarships, allowances, etc. to your bank account;
- signature;
- civil status records;
- health insurance code (CPAM);
- telephone/fax number;
- mobile phone number;
- address (domicile/residence);
- e-mail address;
- profession and/or job;
- vocational training - diplomas - studies;
- data from the medical and sick leave certificates issued;
- where appropriate, other data necessary for the fulfillment of the above-mentioned purpose, according to the legislation in force (unique student code).

**2.3.** The processing of personal data referred to in p. 2.2 will be carried out for the following purposes:

- a) Processing of information on changes in the processing of personal data concerning students which have an impact on the performance of studies;
- b) Enrolment on budget-funded, fee-paying places where applicable;

	<b>Regulation on the processing of information containing personal data in the university management information system "dean's office" (student records)</b>	<b>Code: REG-0- PIDCPSIMUD</b>
		<b>1st edition</b>
		<b>Revision 0</b>

- c) Processing student medical certificates and sick leave certificates in paper only;
- d) Drawing up, recording and processing orders relating to students;
- e) Submission to the CNAM and to the Territorial Military Centers of the nominal records of new students and those who have been dismissed, in paper and electronic format;
- f) Recording and processing student records;
- g) Completion of monthly, quarterly and annual statistical reports on TUM students;
- h) Issuing certificates attesting UTM student status, upon request;
- i) Keeping students' personal files;
- j) Other purposes, necessary for the performance of human resources management activities.

**2.4.** The personal data subject to this Regulation will be stored by those responsible within the UTM in such a way as to allow the identification of data subjects strictly for the period necessary to achieve the purposes for which the data are processed, and at the expiration of that period, the records will be archived, depending on the medium on which they were made. In the case of obligations expressly laid down by law, they may remain in storage and be given the status of archive documents.

**2.5.** Any use of personal data entered in SIMU "Dean's Office" for purposes other than those mentioned above is prohibited.

### **III. LOCATION AND DESCRIPTION OF SIMU "DEAN'S OFFICE"**


**3.1.** The personal data contained in the SIMU "Dean's Office" within the TUM are processed and stored:

- 1. on paper;
- 2. in electronic format:
  - a) Software - SIMU "Dean's Office", which is installed on the computers of all operators responsible for information management within the deanships, departments and other responsible divisions;
  - b) Hardware - computers, which are located in Dean's Offices, departments and other responsible divisions.

**3.2.** The maintenance of the record-keeping software is performed by the employees of the Design and Development of Information Systems and Software Products Service of the Information and Communication Technology Department of TUM, with the following tasks:


- Making adjustments to the program, based on changes in Moldovan legislation;
- Eliminate errors in program operation;
- Consultation in resolving difficulties in using the program;
- Examination of requests received from deans, chairs/departments and other responsible divisions;
- Database management;
- Review and non-disclosure of information with limited accessibility that has become known in the provision of these services.

**3.3.** The processing of information in SIMU "Dean's Office" on paper is structured according to the "folders-folders" criterion, being kept on folders, which are physically located in the office of the Student Records Department at the TUM headquarters.

	<b>Regulation on the processing of information containing personal data in the university management information system "dean's office" (student records)</b>	<b>Code: REG-0- PIDCPSIMUD</b>
		<b>1st edition</b>
		<b>Revision 0</b>

## **VI. PERSONAL DATA PROCESSING PROCEDURE**

- 4.1.** UTM recognizes and respects the right to intimate, family and private life, the processing of personal data being carried out in accordance with the legal provisions in force.
- 4.2.** The personal data of pupils, students, master's and doctoral students are processed/stored: on paper and in electronic format (software and hardware). Exceptions are special category personal data, i.e.: data concerning health status, social affiliation and ethnic origin, which will be processed by UTM on paper only.
- 4.3.** The data processing is done by the software: "Dean's Office", and its maintenance is carried out by the Department of Information and Communication Technologies, TUM.
- 4.4.** The purpose of processing information containing personal data of pupils, students, master's students, doctoral students is to ensure the recording of information related to and necessary for the following processes and activities: admission to studies, registration of pupils, students, master's students, doctoral students, planning and organizing studies, promotion of studies, transfer of students, expulsion and reinstatement to studies, graduation and certification of studies and the submission of activity and statistical reports to state institutions, according to the legislation in force.
- 4.5.** Personal data subject to processing shall be: a) processed fairly and in accordance with the law; b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. The further processing of personal data for statistical, historical or scientific research purposes shall not be considered incompatible with the purpose of the collection if it is carried out in compliance with the legal provisions in force; c) adequate, relevant and not excessive in relation to the purpose for which they are collected and/or further processed; d) accurate and, where necessary, kept up to date. Data which are inaccurate or incomplete in relation to the purposes for which they are collected and/or further processed shall be erased or rectified; e) stored in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are collected and/or further processed.
- 4.6.** The processing of personal data of the candidate is carried out with his/her consent.
- 4.7.** The processing of personal health data is permitted for the management of health services and provision of facilities for students.
- 4.8.** The processing of personal data of pupils, students, master's and doctoral students is carried out by the following subdivisions of TUM: Admissions Commission, Academic Management and Quality Assurance Department, DTIC, Deans of faculties, Technical College. In each subdivision, by order of the Rector of UTM, the persons authorized to process personal data (hereinafter - user) will be appointed, indicating their specific responsibilities.
- 4.9.** Users will only process and access personal data necessary for the fulfillment of their job duties.
- 4.10.** At the end of the processing operations, personal data will be stored in the TUM Archive and in the TUM personal data information system.

	<b>Regulation on the processing of information containing personal data in the university management information system "dean's office" (student records)</b>	<b>Code: REG-0- PIDCPSIMUD</b>
		<b>1st edition</b>
		<b>Revision 0</b>


- 4.11.** Upon expiry of the storage period, personal data will be destroyed in the manner established by law, under the terms set out in Chapter V of this Regulation.
- 4.12.** In accordance with the legislation in force on the protection of personal data, students have the following rights: the right to information, access to data, intervention, objection on personal data concerning them, as well as the right to take legal action.
- 4.13.** All persons involved in the administration and/or processing of information within the study process will respect the procedure for access to personal data.
- 4.14.** Students' right of access to the information concerning them is granted only upon their express written request, with the direct consent of the TUM management. The information provided will be granted in such a way as not to prejudice the rights of third parties. Persons requesting personal data must indicate the purpose of the request as well as the specific period for which they require the information.
- 4.15.** The right of access may be refused where exceptions provided for by law apply. The need to restrict access may arise if there is an obligation to protect the rights and freedoms of third persons, for example, if other persons are included in the information requested and it is not possible to obtain their consent or if irrelevant personal data cannot be extracted by editing.

## **V. STORAGE DURATION**

- 5.1.** The processing of personal data in SIMU "Dean's Office" is carried out during the period of studies at TUM (from the moment of signing the registration order until the student's expulsion). After expulsion it is kept in the Student Records Sector for 3 years from the day of expulsion.
- 5.2.** At the expiration of the deadlines mentioned in point 4.1, the data in the SIMU "Dean's Office" are kept in archived form (on paper) for the period established by the *General Nomenclature of the files of the TUM, approved by the Rector on 17.03.2016*, after which they are subject to destruction or deletion, depending on the medium on which they were made. Electronic data is destroyed after 3 years from the date of expulsion.

## **VI. THE RIGHTS OF STUDENTS AND DATA SUBJECTS**

- 6.1.** TUM, as a personal data controller, guarantees the respect of the personal data protection rights of the students, in accordance with Articles 12-18 of the Law of the Republic of Moldova no. 133 of 08.07.2011, and, where appropriate, other data subjects.
- 6.2.** In accordance with the principles of personal data protection, data subjects benefit from the following rights: the right to information, the right of access to data, the right to intervene, the right to object to personal data concerning them, the right not to be subject to an individual decision, and the right to have recourse to the courts.
- 6.3.** All persons involved in the administration and/or processing of information in SIMU "Dean's Office" will respect the procedure of access to personal data.
- 6.4.** Granting employees (other than executors) the right of access to information concerning them shall be carried out only upon their express written request, with the consent of

	<b>Regulation on the processing of information containing personal data in the university management information system "dean's office" (student records)</b>	<b>Code: REG-0- PIDCPSIMUD</b>
		<b>1st edition</b>
		<b>Revision 0</b>

of the Rector of TUM. The information provided will be provided in such a way as not to prejudice the rights of third parties. Persons requesting personal data must indicate the purpose of the request, as well as the specific period for which they request the information. The purpose of the request must meet the conditions stipulated in paragraph 1 art. 4, paragraph 1 of the Law of the Republic of RM no. 133 of 08.07.2011.

**6.5.** The right of access may be refused where exceptions provided for by law apply. The need to restrict access may arise if there is an obligation to protect the rights and freedoms of third persons, for example, if other persons are included in the information requested and it is not possible to obtain their consent or if irrelevant personal data cannot be extracted by editing.

## **VII. MEASURES TO PROTECT PERSONAL DATA STORED IN SIMU "DEAN'S OFFICE"**

### **7.1. General information security management measures**

7.1.1. In the event of temporary non-use of paper or electronic data carriers containing data taken from the SIMU "Dean's Office", they shall be kept in locations with limited access.

7.1.2. Computers and printers are disconnected from the power supply at the end of work sessions.

7.1.3. The operator shall ensure the security of the points of receipt and dispatch of mail, as well as security against unauthorized access to the copying machines.

7.1.4. Physical access to means of representation of information retrieved from SIMU "Dean's Office" is blocked from unauthorized viewing.

7.1.5. The means of processing information retrieved from the SIMU "Dean's Office" or the software intended for their processing shall be removed from the security perimeter only with the written permission of the Rector.

7.1.6. Removing and introducing information processing means from SIMU "Dean's Office" in/within the security perimeter shall be recorded in the register.

7.2. The measures for the protection of personal data processed in the SIMU "Dean's Office" are carried out taking into account the need to ensure their confidentiality and integrity, through manual, electronic and external protection.


7.3. Special requirements regarding marking: all information output from the SIMU "Dean's Office", containing personal data, shall be subject to marking, indicating the requirements for further processing and dissemination, including the unique identification number of the personal data controller.

7.4. Access to the office where the SIMU "Dean's Office" is located is restricted, being allowed only to persons who have the necessary authorization and only during working hours. Access to the office is possible only with access authorization and the key to the mechanical lock.

7.5. The office is never left unattended when going outside, the office door is padlocked.

7.6. Before granting physical access to the SIMU "Dean's Office", access competences are verified.

7.7. The monitoring registers shall be kept for a minimum of one year, at the expiry of which they shall be liquidated and the data and documents contained in the register subject to liquidation shall be transferred to the archive.

	<b>Regulation</b> <b>on the processing of information containing</b> <b>personal data in the university management</b> <b>information system "dean's office" (student</b> <b>records)</b>	<b>Code: REG-0-</b> <b>PIDCPSIMUD</b>
		<b>1st edition</b>
		<b>Revision 0</b>

7.8. The security perimeter is considered to be the perimeter of the office in which the SIMU "Dean's Office" is located, being physically intact.

7.9. Computers are located in places with restricted access for outsiders.

7.10. Doors and windows are locked if authorized system administration personnel are not in the room.

7.11. The location of SIMU "Dean's Office" responds to the need to ensure their security against unsanctioned access, theft, fire and other possible risks.

7.12. Electrical safety: the safety of the electrical equipment used to maintain the functionality of the SIMU "Dean's Office", of the electrical cables, including their protection against damage and unsanctioned connections, is ensured. In the event of an exceptional situation, breakdown or force majeure, the possibility of disconnecting the electricity to the SIMU "Dean's Office", including the possibility of disconnecting any TIC component, shall be ensured.

7.13. The computers, where the SIMU "Dean's Office" is physically located, are equipped with UPSs, which are used for the correct termination of the working session of the systems (components) in case of disconnection from the power supply.

7.14. Security of network cables: the network cables, through which the data transmission operations retrieved from the SIMU "Dean's Office" are carried out, are protected against unsanctioned connections or damage. To exclude interference, the voltage cables are separated from the communication cables.

7.15. Fire safety in SIMU "Dean's Office": the office where the SIMU "Dean's Office" is located is equipped with fire-fighting equipment and complies with the requirements and fire-fighting standards in force.

7.16. Control of the installation and removal of TIC components: the installation and removal of the program, technical and technical program means used within the SIMU "Dean's Office" shall be controlled and recorded. At the expiry of the retention period, the information containing personal data and information carriers shall be destroyed.

## **VIII. SIMU "DEAN'S OFFICE" USER IDENTIFICATION AND AUTHENTICATION**


8.1. The identification and authentication of the users of the information retrieved from the SIMU "Dean's Office" and of the processes executed on behalf of these users is performed.

8.2. All users (including technical maintenance staff, network administrators, programmers and database administrators) have a personal identifier (user ID), which must not contain any user accessibility level flags.

8.3. Passwords are used to confirm the user ID. The use of passwords in the process of ensuring information security: in addition to the requirements for keeping passwords confidential, it is forbidden to write passwords on paper, except in the case of ensuring the security of their safekeeping (placing the entries in a safe). At the time of entry, passwords are not clearly reflected on the monitor.

8.4. The passwords are changed whenever there is any indication that the system or password has been compromised.

8.5. To ensure that each user can be held accountable, individual user identifiers and passwords are used. The possibility for users to choose and change their individual passwords, including the possibility to activate the procedure for keeping track of their incorrect entries, is ensured.

	<b>Regulation on the processing of information containing personal data in the university management information system "dean's office" (student records)</b>	<b>Code: REG-0- PIDCPSIMUD</b>
		<b>1st edition</b>
		<b>Revision 0</b>

8.6. It shall ensure, for a period of 1 */one/* year, the retention of users' previous hashed password histories and the prevention of their repeated use.

8.7. In the event of termination, suspension or modification of the user's employment relationship and, as a result, the new tasks do not require access to personal data, as well as in the event of modification of the user's access rights, misuse of access authorizations received by the user for the purpose of committing a harmful act, absence of the user from the workplace for a long period (more than 2 months), the identification and authentication codes shall be revoked or suspended.

8.8. In order to detect and avoid the granting of unauthorized access rights, the access rights of users to SIMU "Dean's Office" shall be reviewed regularly, every two months at the latest and after any change of user status

8.9. The use of wireless technologies, mobile equipment is authorized by responsible persons.

8.10. There are limits on who is entitled:

a) view the information stored in SIMU "Dean's Office"

b) copy, download, delete or modify any stored information.

8.11. All employees with access rights receive initial training in personal data protection.

8.12. Any activity of disclosing personal data to third parties shall be documented and subject to a rigorous prior analysis of the purpose and legal basis of the intended disclosure of a given volume of personal data.

8.13. Any breach of security regarding SIMU "Dean's Office" is subject to documentation and the person responsible for implementing the security policy is informed about this as soon as possible.

8.14. Before being granted access to the system, users are informed that the use of the SIMU "Dean's Office" is controlled and that their unauthorized use is sanctioned in accordance with civil, contravention and criminal legislation.

## **IX. SECURITY AUDIT IN THE SIMU "DEAN'S OFFICE"**

9.1. Organize the generation of security audit records in the SIMU "Dean's Office" for the events, indicated in the corresponding list, subject to audit.

9.2. The user's login/logout attempts are logged according to the following parameters:

a) date and time of attempted entry/exit;

b) User ID;

c) the result of the entry/exit attempt.


9.3. Recording of attempts to start/terminate the working session of application programs and processes, intended for the processing of SIMU "Dean's Office" information, registration of changes to user access rights and status access objects according to the following parameters:

a) date and time of the start attempt;

b) name/identifier of the application program or process;

c) User ID;

d) the result of the startup attempt.

	<b>Regulation on the processing of information containing personal data in the university management information system "dean's office" (student records)</b>	<b>Code: REG-0- PIDCPSIMUD</b>
		<b>1st edition</b>
		<b>Revision 0</b>

9.4. Recording of attempts to gain access (to execute operations) to applications and processes for the processing of SIMU "Dean's Office" information shall be performed, according to the following parameters:

- date and time of the access attempt (execution of the operation);
- name (identifier) of the application or process;
- User ID;
- protected resource specifications (identifier, logical name, file name, number, etc.);
- type of operation requested (read, write, delete, etc.);
- the result of the attempt to gain access (execution of the operation).

9.5. The registration of changes in user access rights (competences) and status of access objects is performed according to the following parameters:

- date and time of the change of competence;
- ID of the administrator who made the changes;
- User ID and the user's credentials or specifying access objects and their new status.

9.6. The registration of the exit from the SIMU "Dean's Office", the registration of changes in the access rights of the subjects and the status of the access objects shall be performed according to the following parameters:

- date and time of release;
- the name of the information and how to access it;
- specification of the equipment (device) that released the information (logical name);
- ID of the user who requested the information;
- the volume of the document released (number of pages, tabs, copies) and the result of the release - positive or negative.

9.7. Cases of failure of the security audit in the SIMU "Dean's Office" or the completion of the entire volume of memory allocated for storing the audit results are reported to the person responsible for personal data security policy, who takes measures to restore the working capacity of the audit system.


9.8. The results of the security audit in the SIMU "Dean's Office" (information processing operations and means of conducting the audit) are protected against unauthorized access by applying appropriate security measures and ensuring their confidentiality and integrity.

9.9. The minimum period of storage of security audit results in the SIMU "Dean's Office" is 2 /two/ years, in order to ensure the possibility of using them as evidence in case of security incidents, possible investigations or legal proceedings. In the event of prolonged investigations or judicial proceedings, the audit results shall be kept for the duration of the investigation or judicial proceedings.

## X. ENSURING THE INTEGRITY OF INFORMATION IN THE SIMU "DEAN'S OFFICE"

10.1. The identification, logging and removal of software deficiencies in software intended for information processing in SIMU "Dean's Office", including installation of corrections and their renewal packages, protection against infiltration of malware in software, measures ensuring the possibility of automatic and timely renewal of means of ensuring protection against malware and virus signatures.

10.2. Technologies and means of detection of illegal entries are used, which allow monitoring of events and detection of attacks, including ensuring the identification of attempts of unauthorized use of information from SIMU "Dean's Office".

	<b>Regulation on the processing of information containing personal data in the university management information system "dean's office" (student records)</b>	<b>Code: REG-0- PIDCPSIMUD</b>
		<b>1st edition</b>
		<b>Revision 0</b>

10.3. Ensure testing of the correct functioning of the security components of the SIMU "Dean's Office" (automatically - when the system is started, and where appropriate - at the request of the person responsible for the security policy of personal data processing).

10.4. Back-up copies: based on the volume of processing carried out, on an individual basis, the operator shall determine the time interval within which back-up copies of the information in the SIMU "Dean's Office" and the software used for their automated processing shall be made. The backups shall be tested in order to verify the security of the information bearers and the integrity of the information indicated. Procedures for restoring backups shall be regularly updated and tested to ensure their effectiveness.

## **XI. SECURITY INCIDENT MANAGEMENT OF THE SIMU "DEAN'S OFFICE"**

11.1. The people operating the SIMU "Dean's Office" shall undergo, at least once a year, a training on the responsibilities and obligations in case of execution of actions for management and response to security incidents.

11.2. Security incident handling includes detecting, analyzing, preventing, preventing the development, removing and restoring security. Security incidents are continuously monitored and documented in SIMU "Dean's Office".

11.3. Persons who are guilty of violating the rules on obtaining, storing, processing and protection of information from SIMU "Dean's Office" bear civil, administrative and criminal liability.

## **XII. FINAL PROVISIONS**

12.1. These Regulations are approved by the TUM Senate and revised, if necessary, in case of changes in the legislation in force.

12.2. This Regulation is supplemented by the provisions of the legislation in force.

12.3. The regulation is brought to the attention of the employees-operators of SIMU "Dean's Office" against signature.

12.4. Amendments and additions to this Regulation shall be made in the manner laid down for its approval.