APPROVED AT TUM SENATE MEETING
OF 24.11.2015, MINUTES NO 3

REGULATION ON THE PROCESSING OF INFORMATION CONTAINING PERSONAL DATA IN THE ACCOUNTING SYSTEM OF THE PUBLIC INSTITUTION "TECHNICAL UNIVERSITY OF MOLDOVA"

I. GENERAL PROVISIONS

1. The Regulation on the processing of information containing personal data in the accounting system (hereinafter the Regulation) is developed in order to implement within the Technical University of Moldova (hereinafter the University) the provisions of Law no. 133 of July 8, 2011 on the protection of personal data, the Accounting Law no. 113 of April 27, 2007 and the Requirements for ensuring the security of personal data when processing them in the information systems of personal data, approved by Government Decision no. 1123 of December 14, 2010, and in compliance with the provisions of Articles 91 - 94 of the Labor Code of the Republic of Moldova.

2. This Regulation regulates the general conditions and requirements for the processing of personal data of University employees within the accounting system.

II. PURPOSE OF PROCESSING INFORMATION CONTAINING PERSONAL DATA IN THE ACCOUNTING SYSTEM

3. The purpose of processing information containing personal data in the accounting system is to ensure the recording of accounting information related to the calculation of employees' salary entitlements, including bonuses, incentives, bonuses, allowances, indemnities, compensation and other rights and obligations with pecuniary content, as well as the submission of quarterly and annual financial reports to state institutions, according to the legislation in force.

4. The following categories of personal data are processed in the accounting system:

- ✓ first name, surname and patronymic;
- ✓ State personal identification number (IDNP);
- ✓ date of birth and domicile;
- ✓ personal social insurance code (CPAS);
- ✓ data on the place of employment and the position held;
- ✓ gross salary and other bonuses, bonuses, incentives, supplements;
- ✓ data on family situation (at the request of the applicant);
- ✓ the name, surname, first name (patronymic, if applicable) of the dependants (family members, other relatives and persons, if applicable);

- ✓ data for the transfer to the bank account of salary payments and other amounts due as allowances, compensations or other benefits, as appropriate;
- ✓ the data from the certificates of sick leave granted, necessary to calculate the corresponding allowance;
- ✓ the actual amount of the calculated wage entitlements, related taxes and duties, including compulsory social security contributions for health and social assistance, and other amounts due by virtue of the law or the contract;
- ✓ where appropriate, other data necessary for the fulfillment of the aforementioned purpose, in accordance with the legislation in force.

5. The processing of personal data will be carried out for the following purposes:

a) processing of information on changes in the processing of personal data concerning employees that have an impact on the calculation of salary payments, for example: changes in the qualification level of civil servants, advancement in salary steps, granting or withdrawing the right of access to state secret, evaluation of professional performance of subdivisions with the award of the bonus for collective performance, seniority in the public service;

b) calculation of monthly salaries, in accordance with the legislation in force of the Republic of Moldova (Law no. 48 of 22.03.2012 on the salary system of civil servants and Law no. 355 of 23.12.2005 on the salary system in the budgetary sector);

c) processing employees' sick leave certificates in order to determine the corresponding allowances;

d) processing copies of the Rector's orders concerning personnel;

e) calculating and withholding taxes related to employee salary payments: compulsory health insurance premiums, contributions to the state social insurance budget, income tax, etc..;

f) calculation and payment of compulsory health care insurance premiums and contributions to the state social insurance budget, related to salary payments - employer's obligation;

g) providing the necessary information for the quarterly reports on compulsory state social insurance contributions (Form 4 BASS) and compulsory health insurance premiums (Form MED 08);

h) quarterly preparation of the insured person's statement REV 5 for each employee and their transmission to the Territorial House of Social Insurance, Buiucani branch in electronic format through SIA E-REPORTING and annually on paper;

i) assisting the process (by providing the necessary information) for periodical (monthly) completion of the report and statement on the income paid and income tax withheld from it;

j) filling in monthly, quarterly and annual reports and submitting them to the State Tax Inspectorate sect. Buiucani (regarding income tax IRV 09, TFD 10, IAL 09, MED 08), as well as the preparation and issuance of information on the income calculated and paid on behalf of the individual and the income tax withheld from these incomes to the University employees;

k) the processing of applications and confirming documents regarding the granting of exemptions from income tax withheld from salary, in accordance with Chapter 4, Title II of the Tax Code;

l) issuing salary certificates at the request of employees;

m) filling in and storing the personal records of income in the form of salary and other payments made by the employer for the benefit of the employee for each year, as well as the income tax withheld from these payments (Annex no. 8 to IFPS Order no. 676 of 14.12.2007).

6. Personal data subject to this Regulation will be stored by the University in such a way as to allow the identification of data subjects strictly for the time necessary to achieve the purposes for which the data are processed, and at the expiry of that period, the records will be destroyed / deleted, depending on the medium on which they were made. In the case of obligations expressly provided for by law, they may remain in storage with the status of archival documents.

7. Any use of personal data entered in the accounting system for purposes other than those mentioned above is prohibited.

III. LOCATION AND DESCRIPTION OF THE ACCOUNTING SYSTEM

8. Personal data contained in the accounting system within the University is processed and stored:

1) on paper;

2) in electronic format:

a) Software - Accounting system in the budgetary sphere 1C: Budget, version 8.2., which is installed on the central computer - "Chief Accountant" and with access rights to the second computer - "Materials", computers located in office 115 of the University's study block no. 1, located at the address. Chisinau, bd. Ștefan cel Mare și Sfânt, 168;

b) Hardware - computer inventory no. 1370404, located: bd. Ștefan cel Mare și Sfânt, 168, office 315.

9. The maintenance of the accounting program 1C: Budget is performed by the company "Prima Soft" SRL, being concluded annually a low-value contract on the provision of service between the University and "Prima Soft" SRL, with the following tasks set out the service provider company:

- making adjustments to the program based on changes in the legislation of the Republic of Moldova;
- elimination of errors in program operation;
- consultation in resolving difficulties in using the program (Hotline);
- examination of requests received from the University;
- Examination of the University database (if necessary);
- on-site visits at the request of the University;
- examination and non-disclosure of information with limited accessibility that has become known when providing these services.

10. The processing of information in the paper-based accounting system is structured according to the "folders-folders" criterion, being kept in cabinets, which are physically located in the office 1- 329 of the University, mun. Chisinau, bd. Ștefan cel Mare și Sfânt, 168.

IV. STORAGE DURATION

11. The processing of personal data in the accounting system is carried out during the period of validity of public procurement contracts, during the period of activity of the University's employees (from the moment of signing the contract until the completion of the actions provided for by the legislative acts in the event of termination of employment).

12. Upon expiration of the deadlines mentioned in paragraph 11, the data in the accounting system shall be kept in archived form, for the period established by the Nomenclature of files within the University, approved by the Rector and coordinated with the National Archives of the Republic of Moldova, and subsequently subject to destruction or deletion, depending on the medium on which they were made.

V. RIGHTS OF EMPLOYEES AND DATA SUBJECTS

13. The University, as personal data controller, shall ensure that the personal data protection rights of employees and, where applicable, other data subjects are respected.

14. In accordance with the principles of personal data protection, data subjects have 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 and the right to have recourse to the courts.

15. All persons involved in the management and/or processing of information in the accounting system shall respect the procedure for access to personal data.

16. Employees' right of access to information concerning them shall be granted only by express written request, with the direct consent of the University 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.

17. The right of access may be refused where exceptions provided for by law apply. The need to restrict access may arise if there is a n 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.

VI. PROTECTION MEASURES FOR PERSONAL DATA PROCESSED IN THE ACCOUNTING SYSTEM

18. General information security management measures

18.1. Where paper or electronic data carriers containing data taken from the accounting system are temporarily not used, they shall be kept in locked safes.

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

18.3. 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.

18.4. Physical access to the means of representation of the information retrieved from the accounting system shall be blocked against unauthorized viewing.

18.5. The means of processing information retrieved from the accounting system or the software intended for their processing shall be removed from the security perimeter only with the written permission of the controller.

18.6. The removal and introduction of information processing means from the accounting system from/into the security perimeter shall be recorded in the register.

19. The measures for the protection of personal data processed in the accounting system shall be carried out taking into account the need to ensure their confidentiality and integrity, through protection in manual, electronic and external form.

20. Special requirements for marking: all information output from the accounting system 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.

21. Access to the office where the book-keeping system is located is restricted to persons with the necessary authorization and only during business hours. Access to the office is only possible with access authorization and the key to the mechanical lock.

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

23. Before granting physical access to the book-keeping system, access credentials shall be verified.

24. 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.

25. The security perimeter shall be considered to be the perimeter of the office in which the accounting system is located and shall be physically intact.

26. The security perimeter of the building and office where the accounting system is physically located is inspected daily.

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

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

29. The location of the book-keeping system responds to the need to ensure their security against unauthorized access, theft, fire, flood and other possible risks.

30. Electrical security: the security of the electrical equipment used to maintain the functionality of the book-keeping system, electrical wiring, including their protection against damage and unsanctioned connections. In the event of exceptional circumstances, breakdown or force majeure, the possibility of disconnection of electricity to the accounting systems, including the possibility of disconnection of any IT component, shall be ensured.

31. The computers, where the bookkeeping system is physically located, are equipped with UPSs, which are used for the proper termination of the working session of the systems (components) in case of disconnection from the power supply.

32. Security of the network cables: the network cables, through which the transmission of data retrieved from the accounting system is carried out, are protected against unsanctioned connections or damage. To exclude interference, the voltage cables are separated from the communication cables.

33. Fire safety of the accounting system: the office where the accounting system is located is equipped with fireproof equipment and complies with the requirements and fire regulations in force.

34. Control of the installation and removal of IT components: control and record of the installation and removal of program, technical and technical program means used in the accounting system shall be carried out. At the expiry of the retention period, the information, containing personal data and contained on the information carriers, shall be destroyed.

VII. IDENTIFICATION AND AUTHENTICATION OF THE ACCOUNTING SYSTEM USER

35. The identification and authentication of the users of the information retrieved from the accounting systems and of the processes performed on behalf of these users is performed.

36. 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 signals.

37. 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.

38. Change passwords whenever there is any indication that the system or password has been compromised.

39. 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 a record of their incorrect entries, is ensured. After three failed login attempts, access is blocked, in an automated way.

40. 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.

41. 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 3 months), the identification and authentication codes shall be revoked or suspended.

42. The administration of the access accounts of the users processing personal data in the accounting system, including their creation, activation, modification, revision, deactivation and deletion, shall be carried out by automated support means. The access accounts of temporary users, who process personal data recorded in the accounting system, shall automatically cease to be active at the expiry of the period of time set (for each type of access account). The access accounts of non-active users processing information in the accounting system shall be automatically deactivated after a period of maximum 1 /month/ month. Automated means of recording and informing about the creation, modification, deactivation and termination of access accounts shall be used.

43. In order to detect and prevent the granting of unauthorized access rights, the access rights of users to the accounting system shall be reviewed regularly, at most every six months and after any change of user status.

44. The use of wireless technologies, portable and mobile equipment shall be authorized by responsible persons.

45. There are limits on who is entitled:

a) view information stored in the accounting system;

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

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

47. 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.

48. Any breach of security in relation to the book-keeping system shall be subject to documentation and the person responsible for implementing the security policy shall be informed of it as soon as possible.

49. Before being granted access to the system, users are informed that the use of the accounting system is controlled and that unauthorized use is punishable under civil, contravention and criminal law.

VIII. SECURITY AUDIT IN ACCOUNTING SYSTEMS

50. Organize the generation of security audit records in the accounting system for the events indicated in the corresponding list subject to audit.

51. 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.

52. Registration of attempts to start/terminate the working session of application programs and processes, intended for processing information from accounting systems, registration of changes in user access rights and status of 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.

53. Attempts to obtain access (to execute operations) to applications and processes intended for processing information in the accounting system shall be recorded according to the following parameters:

a) date and time of the access attempt (execution of the operation);

b) name (identifier) of the application or process;

c) User ID;

d) protected resource specifications (identifier, logical name, file name, number, etc.);

e) type of operation requested (read, write, delete, etc.);

f) the result of the attempt to gain access (execution of the operation).

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

a) date and time of the change of competence;

b) ID of the administrator who made the changes;

c) User ID and the user's credentials or specifying access objects and their new status.

55. Logging out from the accounting system, recording of changes in subjects' access rights and the status of access objects shall be performed according to the following parameters:

a) date and time of release;

b) the name of the information and how to access it;

c) specification of the equipment (device) that released the information (logical name);

d) ID of the user who requested the information;

e) the volume of the document released (number of pages, tabs, copies) and the result of the release - positive or negative.

56. The cases of failure of the security audit in the accounting system or of the completion of the entire volume of memory allocated for storing the audit results shall be brought to the attention of the person responsible for the personal data security policy, who shall take measures to restore the audit system's working capacity.

57. The results of the security audit of the accounting records system (information processing operations and means of performing the audit) shall be protected against unauthorized access by applying appropriate security measures and ensuring their confidentiality and integrity.

58. The minimum period of storage of the security audit results in the accounting system shall be 2 /two/ years in order to ensure that they can be used as evidence in the event of security incidents, possible investigations or legal proceedings. If investigations or court proceedings are prolonged, the audit results shall be kept for the duration of the investigation or court proceedings.

IX. ENSURING THE INTEGRITY OF INFORMATION IN THE ACCOUNTING SYSTEM

59. The identification, logging and removal of deficiencies of software intended for processing information in the accounting system, including the installation of patches and their renewal packages, protection against infiltration of malware into the software, measures ensuring the possibility of automatic and timely renewal of the means of ensuring protection against malware and virus signatures.

60. 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 to make unauthorized use of information from the accounting system.

61. Testing of the correct functioning of the security components of the accounting system shall be ensured (automatically - when the system is started up, and, where appropriate - at the request of the person responsible for the security policy for processing personal data).

62. Back-ups: based on the volume of processing carried out, on an individual basis, the operator shall determine the time intervals within which the back-ups of the information in the accounting system and the software used for their automated processing shall be carried out. The back-ups shall be tested in order to verify the security of the information carriers and the integrity of the information indicated. Back-up restoration procedures shall be regularly updated and tested to ensure their effectiveness.

X. SECURITY INCIDENT MANAGEMENT OF THE ACCOUNTING SYSTEM

63. The persons operating the accounting system shall, at least once a year, undergo training on their responsibilities and obligations when carrying out security incident management and response actions.

64. The handling of security incidents shall include detection, analysis, prevention, prevention, removal and restoration of security. Security incidents shall be continuously monitored and documented in the accounting system.

65. Persons found guilty of infringing the rules on obtaining, storing, processing and protecting information in the accounting system shall be liable to civil, administrative and criminal liability.

XI. FINAL PROVISIONS

66. These Regulations shall be reviewed and subsequently approved by the management of the University periodically, but at least once a year, and as necessary.

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

68. The regulations are brought to the attention of employees by publishing them on the University's website.

69. Amendments and additions to this Regulation shall be made in the manner established for its approval.