PRIVATE INSTITUTION OF HIGHER EDUCATION „AMERICAN UNIVERSITY OF MOLDOVA”

REGULATION
CONCERNING THE PROCESSING OF INFORMATION CONTAINING DATA WITH PERSONAL CHARACTER IN THE RECORD SYSTEM CONCERNING STUDENTS

APPROVED
by the University Senate
Americans from Moldova
minutes no. 3 of December 15, 2020
President of the UAM Senate,
Dr., hab., prof.,univ. AVORNIC Gheorghe

_____

CHISINAU 2020

I. GENERAL PROVISIONS

1.1. The Regulation regarding the processing of information containing personal data in the Student students' record system (hereinafter the Regulation) is drawn up in order to implement within the IPÎS "American University of Moldova" (hereinafter the "Operator") the provisions:

- Law no. 133 of July 8, 2011 regarding the protection of personal data
- The requirements for ensuring the security of personal data when processing them within the personal data information systems, approved by Government Decision no. 1123 of December 14, 2010,
- Regulation (EU) no. 679 of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data

1.2. This Regulation establishes the general conditions and requirements for the processing of personal data of the subjects or other persons concerned within the educational process.

1.3. The record system will be notified to the National Center for the Protection of Personal Data (hereafter CNPDCP) to examine its compliance with the legal requirements established in the Law on the Protection of Personal Data. The present Regulation will be attached to the notification to the CNPDCP.

1.4. The regulation will enter into force when its approval is issued by the head of the unit

1.5. The Regulation constitutes an integral part of the Security Policy for the processing of personal data within the Operator and represents the secondary regulatory act that establishes the necessary measures for the processing of personal data of students/masters/doctoral students (hereinafter "subjects").

1.6. This Regulation applies to all personal data processing operations carried out by the Operator in electronic, manual or mixed format, regardless of the software solutions and hardware supports used.

1.7 By operator is meant IPÎS "American University of Moldova", IDNO 1002600041457, with physical address: Chisinau municipality, bd. Ștefan cel Mare și Sfînt, 200, registered at CNPDCP with no. 0003264.

II. PURPOSE OF PROCESSING, CATEGORIES OF PROCESSED DATA AND RECIPIENTS

2.1. The processing of personal data in the record system consists in ensuring the obtaining, keeping, processing, transmission and destruction according to the legislation in force of the personal data of the Subjects.

2.2. The following personal data are processed within the record system

- Name, first name
- No. contact number (telephone/mobile/landline)
- Email

- Domicile
- Signature
- Citizenship
- IDNP
- Date of birth
- The image
- Family situation
- The military situation
- Bank details
- Personal data of family members
- Medical insurance code (CPAM)
- Data from medical certificates
- Ethnic origin
- Data of the legal representative (if applicable)
- Vocational training – diplomas – studies
- Job and/or profession
- Other data necessary to achieve the purposes indicated in this regulation, according to the legislation in force.

2.3. The main operations/sets of processing operations may consist of:

- the collection or registration and organization of personal data
- storing, respectively keeping on any kind of support the collected personal data
- their adaptation or modification or use
- extraction of personal data
- consultation of personal data
- disclosure to third parties by transmission, dissemination or in any other way
- blocking, deleting or destroying personal data.

2.4.Personal data will be processed for the following purposes:

- Carrying out the stages preceding the registration process
- Enrollment of subjects
- the preparation/registration/issuance and processing of different types of documents, aimed at the subjects
- Communication to CNAM and CMT of the nominal record of newly registered subjects, as well as of those who have been deregistered.

- Completion of statistical reports

- Keeping the subjects' personal files

- Preparation of university documents (contract, additional agreements, catalogues, student cards, notes);

- Preparing and issuing study documents (diplomas, certificates, transcripts);

- Issuance of requested documents (student certificate, study certificates);

- Preparation of university reports;

- Photographing or recording audio or video during university activity for teaching purposes and/or for the purpose of promoting and popularizing the image of the University;

- Study fee reductions;

- The safety of students/masters/doctorates and their belongings during the courses (through the video surveillance system of the halls and the university courtyard);

- other purposes, necessary for the execution of the contract, legal obligations or the legitimate interests of the operator.

2.5.Any use of personal data entered in this record system for purposes other than those mentioned above is prohibited, unless there is a reason for this, which justifies this fact.

2.6. Failure to communicate the categories of personal data stated above may lead to the impossibility of realizing certain rights or obligations incumbent on the Operator

2.7. The operator may disclose personal data to:

- the data subject or his legal representative;

- control bodies/state authorities upon their reasoned request;

2.8.Transmission of personal data to other third parties is prohibited.

III. COLLECTION AND PROCESSING OF PERSONAL DATA OF THE SUBJECTS

3.1. Personal data can be collected and processed on the basis of the contract, the legitimate interest and/or consent of the data subject or on the basis of legal provisions.

3.2. Personal data is processed by the data controller in a mixed manner. Manually processed personal data refers to data that can be collected and subsequently processed on paper by filling in forms

3.3. The operator will process mixed personal data, except in situations where the data subject will express his right not to be subject to an individual decision or the right of opposition.

3.4. For the purpose of concluding the contract or its execution, at the request of the data subject, the legal relationship triggered or concluded serves as the basis for the processing of personal data.

3.5. The operator informs that personal data can also be used for other purposes expressly provided for by law, such as: at the request of police bodies or bodies with a control function - activities that the data

operator cannot anticipate, but takes into account at collection of personal data. In the case of such situations, the data operator will verify the correspondence of the request in terms of compliance with the principles of personal data protection and will execute them only in the case of justifying the existence of the purpose and the legal basis.

3.6. The conclusion of contracts with subjects - natural persons is carried out by the Operator's employees, subsequently being entered into the informational resource used by the Operator, to which he has unique access.

3.7. The processing of personal data in this record system is carried out for the following periods:

- For the period of the execution of the contract, from the moment of collecting/obtaining personal data until the termination of the contractual relationship.
- If the legal norms provide for other storage terms (Order No. 57 of 27.07.2016 of the National Archive Agency regarding the Indicator of model documents and retention terms for public administration bodies, for institutions, organizations and enterprises of the Republic of Moldova or other applicable legal acts (as applicable).

If the personal data are processed for the fulfillment of legitimate interests or legal obligations of the Operator, the personal data will be processed for the duration of the time period necessary for their fulfillment.

3.8. In electronic format, the subjects' data using the database created through Microsoft SQL software on the Microsoft Server 2008R2 platform, the data storage servers being located in the office of the Accounting department, access being restricted.

3.9.After the fulfillment of the legitimate purposes of processing and storage and after the expiry of the legal period for the archiving of data/documents containing personal data, if the data subject has not given his consent for further processing and any of the exceptions provided by the protection legislation are not applicable data, proceed as follows:

- personal data from IT record systems/applications will be deleted or
- personal data in the records systems/IT applications will be transformed into anonymous data
- existing data in paper documents will be destroyed with shredders, specially intended for documents classified as confidential/restricted documents.

IV. DATA PROTECTION PRINCIPLES PERSONAL CHARACTER

4.1.The operator is obliged to comply with the legal principles of personal data processing provided by data protection legislation, as detailed below.

4.2. **The principle of the legitimacy of personal data processing**

It establishes the following obligations for the Operator, its employees and collaborators:

4.2.1. Personal data will be processed correctly and in compliance with the law

4.2.2. Personal data will only be processed if the data subject has given his express and unequivocal consent to that processing, or in the case of the applicability of one of the above-mentioned exceptions

4.2.3. Personal data will only be obtained for one or more specific purposes and will not be processed in a way that is inconsistent with those purposes.

Processing for subsequently identified purposes is permitted only in situations where consent is not required, provided that the persons concerned are informed in advance.

4.3. The principle of transparency of personal data processing

The data subject will be informed in advance about the personal data to be processed, the purpose of the processing and its legal basis, the identity of the operator, the legitimate interest pursued by the operator through the processing of personal data, if applicable, the recipients or the categories of data recipients, if applicable, the intention of the Operator to transfer personal data to a third country or an international organization, if the provision of all requested data is mandatory and the consequences of refusing to provide them, the period for which the data will be stored with personal character or, if this is not possible, the criteria used to establish this period, the existence of an automated decision-making process including the creation of profiles as well as, at least in the respective cases, information regarding the logic used, the importance and the expected consequences of such processing for the data subject, the rights of the data subject provided by the legislation in the field of data protection as well as the conditions under which they can be exercised, respectively with regard to any other information specific to the actual processing purpose. Whenever the data subject, whose data is processed, will request information regarding the processing of his data, the department that receives such a request will ask for a point of view from the Data Protection Officer. The operator has the obligation to respond to the above-mentioned requests within 30 days at most from the moment of their receipt, in accordance with the provisions of the data protection legislation.

4.4. The principle of proportionality of personal data processing

The operator processes personal data reasonably, relevant to the purpose of processing and not excessively, limited to what is necessary in relation to the legitimate purposes for which the data are processed.

Before processing personal data, the Operator, through the relevant departments, with the approval of the Data Protection Officer, determines whether and to what extent the processing of personal data is necessary to achieve the purpose for which it was collected.

4.5. The principle of data deletion after the expiry of the legal retention period

With regard to the archiving period of personal data, they will be stored in the Operator's systems for the fulfillment of the legitimate purposes pursued by the processing, for a period necessary for the purpose of the processing or for the period provided by the applicable legislation, for each category of personal data in part. The storage period is established for each identified operation, taking into account the mandatory legal provisions.

The operator has the obligation to keep proof of the existence of the consent expressed by the subjects, if the processing of their personal data is carried out based on their consent.

After the achievement of the legitimate purposes of processing and storage and after the expiration of the legal period for archiving data/documents containing personal data, if the data subject has not given his consent for further processing and any of the exceptions provided by the legislation on the protection are not applicable data, proceed as follows:

- personal data from record systems/IT applications will be deleted or
- personal data in the records systems/IT applications will be transformed into anonymous data
- existing data in paper documents will be destroyed with shredders specially designed for documents classified as confidential/restricted documents.

4.6. The principle of accuracy of personal data processing

Personal data will be accurate and, if necessary, updated. The operator takes the necessary measures to ensure that personal data that is inaccurate is deleted or rectified without delay in accordance with the legitimate purpose of the processing.

4.7. The principle of confidentiality of personal data and the principle of the need to know the data („need to know")

The operator adopts the necessary technical and organizational measures to ensure adequate security of personal data, to prevent unauthorized access, illegal processing, unauthorized disclosure, including their loss, destruction, or accidental damage. Details about the minimum security requirements are also mentioned in the following sections.

The access of the Operator's employees/partners to the personal data processed by the Operator, respectively stored in the Operator's computer systems is granted only on the basis of the "need to know" criterion. There must be a documented authorization and approval process to grant, maintain and remove access to

information that is personally identifiable. Thus, in order to grant the access rights of some subjects, they will submit a request to the studies section in this regard.

4.8. The principle of responsibility in carrying out the processing of personal data

The operator ensures compliance with the legal principles of personal data protection both for the data processing carried out directly, ensuring the inclusion of the contractual clauses provided by the data protection legislation in the contracts concluded with its contractors.

All technical and organizational measures will be applied to prevent unauthorized access, unauthorized and illegal processing of personal data, unauthorized disclosure and destruction, alteration, or accidental loss of personal data.

V. THE RIGHTS OF THE PERSONS CONCERNED

5.1. As a personal data operator, the Operator guarantees compliance with the rights regarding the protection of personal data belonging to the subjects, as well as, as the case may be, to other data subjects.

5.2. In accordance with the principles of personal data protection, the data subjects benefit from the following rights: to information, access to data, intervention, opposition to the personal data concerning them, as well as the right to address in justice.

5.3. All persons involved in the activity of administration and/or processing of information in the record system shall comply with the procedure for access to personal data.

5.4. The granting of employees' right of access to the information concerning the subjects is carried out by express request, in written form, with the direct consent of the management. The information provided will be provided in such a way as not to prejudice the rights of the subjects. Personal data subjects requesting personal data must indicate the purpose of the request, as well as the specific period for which they are requesting the information.

5.5. There is the possibility of denying the right of access in the situation where the exceptions provided by law apply. The need to restrict access may be imposed if there is an obligation to protect the rights and freedoms of third parties, for example, if other persons appear in the requested information and there is no possibility of obtaining their consent or they cannot be extracted, by editing, irrelevant personal data.

VI. Technical and organizational measures implemented by the Operator to ensure data protection from the moment of conception and by default (privacy by design și privacy by default)

6.1. The operator undertakes to protect the personal data of the data subjects that have been processed as a result of interactions with them, as well as with any other natural persons.

6.2. Taking into account the nature, scope, context and purposes of the processing, as well as the rights and freedoms of the natural persons concerned, the Operator implements appropriate technical and organizational measures" to guarantee and be able to demonstrate that the processing of personal data is carried out in accordance with the legislation in force, both national and European. These measures are periodically reviewed by the Data Protection Officer, IT Department, Security Department and updated in accordance with applicable legal requirements.

6.3. Organizational measures:

- Access to the security perimeter of the personal data operator is prohibited, except in cases of authorized control.
- The employees of the personal data operator have the right to have access to the spaces and/or locations for which they have the administrator's consent. The access of other people to the security perimeter can only take place under the supervision of employees. Law enforcement bodies or control bodies may have access to the security perimeter in case of the existence of appropriate powers of attorney (in original), copies of which are provided to the operator's representatives;
- The headquarters where the means of personal data processing are located is physically intact. The outer walls of the rooms are resistant, the entrances are equipped with locks. The keys to the door locks are kept by the administrator. The administrator keeps track of the keys and the people who have access to the security perimeter of the personal data operator. The doors and windows in the security perimeter are locked when employees leave the premises;
- The use of photo, video, audio or other means of recording in the security perimeter is only allowed if there is permission from those in charge;
- If the employee's employment contract has terminated or been suspended, the administrator of the personal data operator is obliged on the same day to withdraw the keys from the access ways as well as from the cabinets or metal safes, such as and computer access rights;
- Before taking up the position, all employees are made aware of the Security Policy under their signature, including signing the non-disclosure clause of the information with limited accessibility that they will come into possession of within the operator in the context of the exercise of the tasks and predetermined attributions. The disclosure of personal data or other confidential information by means of electronic means to unidentified persons is not allowed;
- In case of temporary non-use of information carriers on paper or electronic (digital) media containing personal data, they are kept in a specially designed space that can be locked. Computers, access terminals and printers are disconnected at the end of work sessions.
- The Operator's employees will ensure the implementation of the recommendations received from the Data Protection Officer within the data processing operations they carry out on behalf of the Operator;

- All developments and updates regarding the systems and equipment involved in the processing of personal data will be done in compliance with the principles "data protection by design" and "data protection by default", respectively compliance with the right to data protection starting from the moment of conception and by default ;
- Only the personnel who need to access the personal data for the performance of their job duties shall be authorized to have access to the Operator's databases, systems and applications ("need to know basis" principle).
- Employees and collaborators of the Operator who have received access authorization to databases or who have rights to administer them, respectively the IT systems and applications that store them, will regularly participate in training programs regarding the protection and security of personal data personal.

6.4. Technical measures:
- Personal data will be transmitted only under safe conditions, any transmission of personal data outside the Operator, which does not fall within the provisions approved by the Data Protection Officer, will only be carried out with his prior approval.
- Backups: based on the volume of processing carried out, individually, it is established by the operator in the time interval in which the backup copies of the information from the software used for their automated processing are performed. The backup copies are tested in order to verify the safety of the information carriers and the integrity of the indicated information. Procedures for restoring backups are updated and tested regularly, in order to ensure their effectiveness.
- In the case of personal data processing carried out by the Operator through authorized persons, the Operator will ensure that they also implement appropriate technical and organizational measures in order to ensure an appropriate level of data security, including in the contracts concluded with them clauses regarding the requirements data security minimums regarding the appropriate technical and organizational measures identified.
These measures may include, but are not limited to:
a) Measures regarding minimizing the amount of personal data through filtering and elimination, reducing sensitivity through conversion, reducing data accumulation, restricting access, reducing the ability to identify the nature of the data, according to the Operator's instructions.
b) Traceability measures – the existence of a traceability and log management policy, with their retention for the entire duration of the data processing operations, but at least 2 years.
c) Measures regarding the relations of Authorized Persons with subcontractors - the existence of regulations and processes to reduce the risks of unauthorized access to data.

d) Measures for the deletion, anonymization and/or return of personal data by the authorized person after completion of processing on behalf of the operator, except for situations where there is a legal requirement to store personal data and after completion of processing.

- The operator keeps track of the computing devices that store personal data and other managed confidential information;
- It is forbidden to use personal computing devices such as: laptop, tablet, media sticks, etc. for the purpose of carrying out the tasks of the personal data operator;
- Access to the computers is based on a user profile and password that is confidential and cannot be transmitted to anyone or transcribed or displayed for unrestricted access. Passwords contain at least 8 symbols, which are not related to the user's personal information, do not contain consecutive identical symbols and are not entirely composed of groups of numbers or letters. Passwords will change over 3-month intervals;
- The computing devices are equipped with an antivirus program and licensed operating systems;
- The computing devices for each user are individually configured with access and use filters of the hardware support depending on its tasks and functional attributions;
- It is forbidden to remove information with limited accessibility from the security perimeter without a permission from the data operator;
- It is forbidden to use remote access programs to the computing technique.
- Technical and administrative conditions of electrical and fire safety are ensured;
- In the case of extracting personal data, the documents are marked, indicating prescriptions for further processing and its dissemination, including indicating the unique identification number of the personal data operator according to the warning model: "The document contains accessible information limited. Operator registered/authorized by the National Center for the Protection of Personal Data with no. XXXXXX from www.registru.datepersonale.md

.

VII. The person responsible for the protection of personal data

7.1. Responsible for ensuring the personal data protection regime within the records system is the Administrator, who has the necessary knowledge, administrative resources (time, human resources, equipment and budget) and has free access to the information necessary for the performance of his functions.
7.2. The data protection officer has at least the following tasks:

a. informing and advising the Operator as well as the employees dealing with the processing regarding their obligations regarding the protection of personal data

b. monitoring compliance with legal provisions related to data protection and the Operator's policies regarding the protection of personal data and providing consultancy and recommendations to the Operator and its internal departments to ensure compliance with obligations in the field of data protection

c. providing support in the development of internal policies and procedures that are necessary for the internal regulation of personal data processing operations

d. providing advice upon request regarding the assessment of the impact on data protection and the monitoring of its operation (gives an opinion in the case of personal data processing operations subject to impact assessment, regarding the Operator's obligation to carry out this analysis, the methodology that is to be used, the existence of the necessary resources, the security, technical and organizational measures to be applied to reduce the risks to the rights and freedoms of the data subject; issues opinions on the correctness of the manner in which the impact analysis was carried out and on its conclusions, giving an opinion positive or negative regarding the performance of the processing operation)

e. is the contact person of the operator in the field of personal data protection, being mentioned in the information of the concerned persons

f. is the operator's contact person in the relationship with the CNPDCP in the case of controls carried out by it, as well as in the case of its prior consultation.

g. cooperation with the supervisory authority

h. assuming the role of point of contact for the supervisory authority regarding aspects related to processing

i. participation in professional training programs for knowledge of legislation and practice in the field of data protection

7.3. The operator publishes the contact details of the data protection officer and communicates them to the supervisory authority.

VIII. DATA PROTECTION AND SECURITY INCIDENTS

8.1. Incidents of IT systems affecting personal data of subjects or other data subjects are considered high risk incidents.

8.2. In the event of a personal data security incident, the provisions of the Policy regarding security incidents with an impact on the protection of personal data will also be taken into account.

8.3. The effects of personal data security incidents for the data subject may consist of: physical, material and moral damages, discrimination, identity theft or fraud, reputational compromise, loss of confidentiality of personal data protected by professional secrecy, or any other significant disadvantage of an economic and social nature, including but not limited to the deprivation of his rights or the impossibility of exercising control over his personal data.

8.4. Examples of personal data security incidents:

-theft or loss of a laptop or external memory containing personal data of the subjects;

- the personal data of the subjects who used the enrollment service through the mobile application/website are accessed by exploiting a vulnerability of the application;

-an e-mail with sensitive information sent to a recipient other than the intended recipient, etc.

- unauthorized access to the internal network of the Operator;

- transmission of personal data to personal email addresses

8.5. In the situation where an IT security incident affects personal data, the IT Department or the Operator's employee who took note of such an incident, will immediately inform the Data Protection Officer for the analysis of the immediate measures to be taken by the Operator as would be the notification of the CNPDCP regarding the incident within 72 hours from the date on which the Operator's employee became aware of it and/or the notification of the persons concerned in the event of the existence of a high risk regarding their rights and fundamental freedoms.

8.6. The notification sent to the CNPDCP by the Data Protection Officer in the event of such an incident:

- describe the nature of the breach of personal data security, including, where possible, the categories and approximate number of data subjects in question, as well as the categories and approximate number of personal data records in question;

- communicate the name and contact details of the data protection officer or another point of contact where more information can be obtained

- describes the probable consequences of the breach of personal data security

- describes the measures taken or proposed to be taken by the Operator to remedy the problem of the personal data security breach, including, as the case may be, the measures to mitigate its possible negative effects.

8.7. Also, any other type of incident that could affect personal data processed by the Operator, will be brought to the attention of the Data Protection Officer for analysis in accordance with the legislation on the protection of personal data.

8.8. If there is a security incident likely to generate a high risk for the rights and freedoms of natural persons, the Operator will inform the affected person without undue delay about this incident.

8.9. Annually, by January 31, the holders of personal data submit to CNPDCP the generalized report on security incidents of personal data information systems. Based on this report, the Center undertakes the measures required by the Law regarding the protection of personal data.

IX. RESPONSIBILITY FOR NON-COMPLIANCE WITH THE PROVISIONS REGARDING THE PROCESSING OF PERSONAL DATA

9.1. For non-compliance with the provisions of this Regulation, the guilty persons shall be held liable for disciplinary, contraventional, criminal or material liability, as the case may be.

X. FINAL PROVISIONS

10.1. These Regulations are revised and subsequently approved by the management of the Operator, periodically, as well as when necessary.

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

10.3. The modification and completion of this Regulation is done in the manner established for its approval.