INTERNAL RULES FOR DATA PROTECTION

Approved May 21, 2018

These internal rules for data protection represent the principles and legal conditions which the American University in Bulgaria (AUBG) shall observe when it receives, processes, transfers or keeps personal data for the purposes of its activity, including personal data of candidate students, students, alumni, clients, suppliers, employees and workers. The rules comply with the requirements of the General Data Protection Regulation (Regulation 2016/679) (GDPR).

1. Interpretation

1.1. Definitions

Automated taking of decisions: when a decision is fully taken on the basis of automated processing (including profiling) and it leads to legal consequences or it significantly affects the natural person. GDPR forbids the automated taking of decisions (unless certain conditions are present), as this does not concern the automated processing.

Automated processing: any form of automated processing of personal data, consisting in the use of personal data for the purpose of evaluating the personal aspects of a given natural persons, in particular analysis or prognosis of different aspects which relates to the work results of the data subject, the economic condition, health, personal preferences or interest, reliability or behavior, location or movements. Profiling is a type of automated processing.

Administrator: the person or organization which determines when, why and how personal data is processed. The administrator is responsible for specifying practices and policies in compliance with GDPR. The American University in Bulgaria is an administrator of all personal data which concerns the candidate students, students, alumni, clients, suppliers, employees and workers.

Data protection officer (DPO): the data protection officer (DPO) is responsible for the control over the application of these rules, as well as, if applicable, for the development of connected policies and other terms of reference. This position is now held by Margarita Petkova, with address: 1 Georgi Izmirliev Square, town of Blagoevgrad, contact number:
073 888 337, dpo@aubg.edu.

European Economic Area (EEA): it includes those 28 countries which are member states of the European Union, as well as Iceland, Lichtenstein and Norway.

Data protection at the stage of planning: introduction of appropriate technical or organizational measures in an effective way which shall provide compliance with GDPR.

Data protection notifications: separate notifications which include information that is provided to the data subjects at the time when AUBG collects information about them. These notifications can be both common (for example, addressed to workers and employees or notifications on the website) and relating to processing with a specific purpose.

Explicit consent: consent which requires a very clear and definite statement (not just an action).

Name of the organization: American University in Bulgaria, American University Service Company, American University in Bulgaria.

Personal data: any information that identifies a data subject or information that is connected with a data subject, as we can identify (directly or indirectly) these subjects only on the basis of the data or in combination with another identifiers which we posses or in respect of which we have access to. Personal data includes "sensitive personal data" and pseudonymised personal data, as it excludes anonymised personal data. Personal data can refer to facts (for example – name, e-mail, location or date of birth) or information concerning the actions or behavior of the data subject.

Personal data protection breach: any action or inaction that compromises the security, confidentiality or integrity of the data, or of the natural, technical, administrative or organizational protections which we or our subcontractors use in order to protect personal data. The loss, unauthorized access, provision or receiving of personal data are examples of security breach.

Data processing: any action which is connected with the use of personal data. This includes: receiving, saving, keeping, performing an operation or a series of operations with the data, for example, organization, editing, restoration, using, provision, erasure or destruction. Processing also includes the transfer of personal data to third parties.

General Data Protection Regulation: the General Personal Data Protection Regulation ((EU) 2016/679). Personal data are subject of the protection that is given in GDPR.

Impact assessment: mechanisms and measures used for identification of the risk relating to the processing of data. The impact assessment shall be made for all key systems or programs connected with the processing of personal data.

Staff: all workers and employees.

Pseudonymization: the replacement of information which directly or indirectly identifies a natural person, with one or more artificial identifiers ("pseudonyms"), so that the person cannot be identified without access to the additional information which shall be separately kept and which shall be confidential.

Data subject: an identified natural person or a natural person who can be identified and whose personal data is processed by AUBG.

Consent: any freely given, concrete, informed and unambiguous indication for the will of the data subject, as the same is given through a statement or clearly confirming action which expresses consent for processing of personal data connected with it.

Sensitive personal data: information which reveals the racial or ethnical origin, political opinions, religious or other similar beliefs, membership in trade-unions, physical or mental health condition, sex life, sexual orientation, biometric or genetic data, as well as personal data concerning criminal offences and sentences.

2. Introduction

This data protection policy regulates the management of AUBG in respect of the personal data which relates the candidate students, students, alumni, clients, suppliers, employees, workers and other third parties.

These internal rules are applied in respect of all personal data which AUBG processes, regardless of the mean it is stored on and the category of data subjects it is connected.

These internal rules shall be applied in respect of the whole staff of AUBG. All workers and employees shall read, get acquainted with this policy and comply with it when processing personal data on behalf of AUBG, as they also shall be present during trainings when it is necessary and predicted by AUBG.

These rules represent an internal document and they cannot be shared with third parties, clients or regulatory authority without the prior consent of AUBG.

3. SCOPE

The right and lawful management of personal data will provide the trust in AUBG on behalf of candidate students, students, alumni, clients, suppliers, employees, workers and partners.

The protection of confidentiality and integrity of personal data is a key responsibility in respect of which AUBG behaves really serious. The organization can be subjected to a sanction in amount of 20 million euros or 4% of the world turnover (whichever of these two is higher and depending on the concrete breach), if it does not observe the requirements of GDPR.

All leaders and managers of departments bear responsibility for the observance of these rules on behalf of the staff and they shall introduce relevant practices, processes and training.

The data protection officer (DPO) is responsible for the control which relates to the application of these rules, as well as, if applicable, for the development of connected policies and other instructions. At the moment this position is held by Margarita Petkova, address: 1 Georgi Izmirliev Square, town of Blagoevgrad, contact number: 073 888 337, dpo@aubg.edu.

Please, contact the data protection officer in case of any enquiries relating to the application of these rules or if you have any fears that the same are not correctly applied. It is obligatory for you to contact the data protection officer in the following situations:

- If you are not sure about the legal basis which you can rely on in respect of the processing of personal data (see section 5.1 below);
- If you need to be given consent and/or if you have to provide explicit consent;

- If you have to prepare data protection notifications (see section 5.3 below);
- If you have any concern in connection with the term for keeping personal data which you process;
- If you are not sure about the data security measures which you have to introduce in order to protect personal data;
- If you found a breach of the protection of personal data;
- If you are not sure on what a basis you can make a transfer of personal data out of the European Economic Area (see section 11 below);
- If you need cooperation because of a given information that a data subject wants to exercise some of his/her rights in compliance with GDPR (see section 12 below);
- Always when you plan to begin or to significantly change the way you perform a concrete operation relating to the processing and which can require impact assessment (see section 13.5 below) or when you have the intention to use personal data for purposes which are different of those for which it is collected;
- If you plan to carry out activities relating to the processing of personal data, based on automated processing, including profiling and automated taking of decisions;
- If you need cooperation in respect of the observance of the applicable law and in connections with activities which concerns direct marketing (see section 13.6 below);
- If you need cooperation in connection with trade or other contracts, or in other spheres in connection with the sharing of personal data (see section 13.7 below).

4. Principles for protection of personal data

AUBG abides by the principles for protection of personal data mentioned in GDPR and which require all personal data:

- To be processed legally, conscientiously and clearly;
- To be collected only for concrete, specially specified and legitimate purposes;
- To be appropriate, connected with and limited to what is strictly needed for the purposes they are processed for;
- To be true and if it is possible to be actual;
- To be stored in a form which can allow the identification of the data subject for not a longer period than the one which is necessary for the purposes of the processing;
- To be processed in a way which provides their security, using technical and organizational measures which shall protect it against unauthorized or illegal processing and against accidental loss, destruction or damage;
- Not to be transferred to another country out of the European Economic Area without the necessary protection measures;
- To be provided to the data subjects who shall be given an opportunity to exercise their rights in respect of their personal data.

At any time AUBG shall be able to prove that it complies with the principles which are given above.

5. Conformity with the law, conscientiousness, clarity

5.1. Conformity with the law and conscientiousness

Personal data shall be processed in conformity with the law, conscientiously and in a clear way in respect of the data subject.

GDPR limits the circle of actions with personal data to those for which there is a legal basis. These limitations do not aim to prevent processing but to guarantee that the personal data is processed conscientiously and without negative consequences for the data subject.

GDPR regulates the legal bases for processing, as some of them are given below:

- The data subject has given his/her consent;
- The processing is necessary in connection with the performance of a contract concluded with the data subject or for the initiation of steps because before the conclusion of the contract and at the request of the data subject;
- Processing is necessary in order to be fulfilled a legal obligation of AUBG;
- Processing is necessary in order to be protected essential interests of the data subject;
- Processing is necessary in order to be executed a task that is off public interest;
- Processing is necessary for the purposes of the legitimate interests of AUBG, except when the interests or the main rights of the data subject have advantage over these interests. The purposes in respect of which AUBG processes personal data because of this have to be described in the applicable notifications about the data to the respective groups of data subjects.

5.2. Consent

The data administrators can process personal data only in the cases when at least one of the legal bases of GDPR is present and which also includes “consent”.

The data subject agrees with the processing if he/she expresses it clearly – through a declaration or a positive act. This consent requires a positive action – previously selected consent fields and inaction do not represent valid consent. If the consent for processing personal data is given with a document, then it shall be required apart from the consent with the other issues.

The data subjects shall easily withdraw their consent for the processing at any time and the withdrawal shall be taken into consideration in due time. The consent shall be again required if you intend to process personal data on the basis of a new, different reason in respect of which the subject has not given his/her initial consent.

In the cases when AUBG cannot rely on another legal basis for processing, the explicit consent is usually necessary in cases of processing sensitive personal data, automated taking of decisions, data transfer out of the European Economic Area and etc.

Whenever it is relied on consent, this has to be proved by documents and the respective records have to be kept in order AUBG to demonstrate the compliance with the requirements concerning the receiving and keeping of consent.

5.3 CLARITY IN RESPECT OF THE DATA SUBJECT

GDPR requires all the administrators to provide the data subjects with detailed and correct information depending on whether the data are received directly by them or by another source. This data has to be provided by proper data protection notifications which shall be easily accessible and shall use clear language without any unnecessary legal terminology, so that the data subjects to be able to understand them.

Whenever we collect personal data directly from the subject, including with the purpose of administration of employment relationships, we shall provide them the information which is required by GDPR.

The information shall include: information for contact with the administrator and the data protection officer, how and why personal data is collected, processed provided, protected and kept. AUBG has the obligation to provide this information at the time of receiving personal data from the subject.

6. Limitation of the purposes

All personal data has to be collected only for concrete and legitimate purposes and it does not have to be processed in a way that is not compatible with these purposes.

You do not have the right to use personal data for new, different and incompatible with the initial purposes, unless the subject provides consequent consent for the new purposes.

7. Data minimization

The personal data shall be appropriate, connected with and limited to what is strictly necessary for the purposes for which it is processed.

The employees and workers of AUBG have the right to process personal data only when this is connected with the performance of their official duties. It does not have to be collected personal data when the same is not necessary.

Each employee who works with personal data is engaged to provide timely deletion/destruction or anonymization, in compliance with the instructions of AUBG, of all personal data that is not necessary anymore for the concrete purposes in respect of which it is collected.

8. Correctness

The personal data shall be correct and if it is possible it shall be maintained in actual form. In case of an error, the data shall be corrected or deleted without any delay.

Each employee shall be sure that the personal data which it keeps is correct, complete, actualized and limited to the purposes in respect of which it is collected. The correctness of all personal data has to be checked at the time it is collected and at regular intervals thereafter, as well as all reasonable measures have to be taken for the destruction or correction of all incorrect or irrelevant personal data.

9. Limitation of the keeping

The personal data does not have to be kept in a form which allows the identification of the subject and for time that is longer than the necessary for the purposes in respect of which it is collected.

Each employee who works with personal data shall take all reasonable measures for the destruction and deletion from all systems of all personal data which is not necessary anymore and in compliance with the rules and keeping policies of AUBG – this may include the obligation third parties to be required to delete these personal data.

Each employee shall be sure that the data subjects are informed (through the respective data protection notifications) about the length of the period during which their personal data will be kept and the principle for determination of this period.

10. Security, integrity and confidentiality

10.1. Personal data protection

The personal data shall be protected with the necessary technical and organizational measures against unauthorized and illegal processing, as well as against accidental loss, destruction and damage.

AUBG will work develop, introduce and maintain appropriate protection measures in conformity with the activity, resources, quantity and the type of the personal data which is processed. Regular assessment will be made in respect of the efficiency of these measures. Each employee will also be responsible for the protection of the personal data which AUBG keeps and he/she shall be really careful when he/she protects sensitive personal data against loss and unauthorized access, use or provision.

Each employee shall follow all procedures and technological measures which AUBG has introduced for the purpose of protecting the security of personal data from the moment of its collection to the moment of its destruction. You can transfer personal data to subcontractors only if they agree to observe the same policies and procedures and if they provide the necessary protection measures which AUBG requires.

Each employee has to provide the security of personal data, as he/she shall protect its confidentiality, integrity and accessibility, defined as follows:

- Confidentiality means that only the persons who shall know and are authorized to use personal data have access to the same;
- Integrity means that the personal data are correct and appropriate in order to be used for the purposes in respect of which it is processed;
- Accessibility means that the authorized users are provided with access to personal data for authorized purposes.

Each employee has to observe and it does not have to impede the action of the administrative, physical and technical protections which AUBG introduces.

10.2. REPORTING A BREACH

GDPR requires the administrators to report a breach in respect of data protection to the regulatory authority and in some cases to the data subject.

AUBG introduces procedures for identification of similar breaches and it will inform the regulatory authority and the data subject, if it is necessary, in the predicted by GDPR cases.

Each employee who has information about a breach in respect of the data protection or a suspicion that there is such a breach, he/she has to connect the person or the team that is predicted for the purpose: data protection officer, information security department, legal department. All the evidences for a potential breach have to be kept.

11. Limitation of the transfer

GDPR limits the transfers of data to countries which are out of the European Economic Area with the purpose to guarantee before the subjects that the guaranteed by GDPR protection level is not compromised.

Transfer of personal data out of the European Economic Area can be made only if it is present one of the following conditions:

- The European Commission has passed a decision confirming that the country in respect of which the transfer is made provides adequate protection level in regard to the rights and freedoms of the data subjects;
- There are appropriate protection measures – for example, binding corporate rules (BCR), standard contractual clauses, approved by the European Commission, an approved code of conduct or a certification mechanism;
- The data subject has given his/her explicit consent for the transfer, as this is done after the same is informed about the possible risks or
- The transfer is necessary for one of the purposes which is mentioned in GDPR, including the execution of a contract with the subject, protection of the public interest, ascertainment and protection of legal disputes, protection of the essential interests of the data subject in the cases when the same is physically or legally incapable to give his/her consent, as well as in some limited cases – for protection of our legitimate interests.

12. Right of the data subjects and requests for access to data

The data subjects have rights in respect of the way their personal data shall be managed, including the right to:

- Withdraw their consent for processing, as they can do this at any time;
- Receive concrete information about the actions which relate to the processing on behalf of the administrator;

- Request access to their personal data which is processed;
- Raise an objection against the use of their personal data for the purposes of the direct marketing;
- Request the deletion of their personal data in case that the same is not necessary anymore for the purposes in respect of which it is collected or a correction of incorrect or incomplete data;
- Limitation of the processing in concrete situations;
- Litigation of processing which is performed on the basis of protection of legitimate interests or public interest;
- Request a copy of the contract on the basis of which their personal data is transferred to a country which is out of the European Economic Area;
- Raise an objection against a decision which is fully taken on the basis of automated processing, including profiling;
- Be informed about a breach against data protection and which can lead to a high risk for their rights and freedoms;
- Lodge a complaint with the regulatory authority;
- In some cases to receive or to request their personal data to be transferred to third country in a structured, generally used form which shall be suitable for machine reading.

Each employee shall verify the identity of the person who wants to exercise some of the given above rights (the employee does not have to allow third parties to receive personal data without prior authorization).

Each employee has to immediately forward any request for access to personal data he/she receives to his/her line manager or to the data protection officer of AUBG.

13. Records

13.1. The administrator shall introduce the necessary technical and organizational measures in an efficient way in order to provide the observance of the principles of data protection. The administrator is responsible for the observance of these principles and he/she shall be able to prove their observing.

The organization has to be posses the necessary resources and control mechanisms in order to provide the observance of GDPR requirements, including:

- Appointment of data protection officer who possesses relevant qualification (if applicable) and assuming managerial responsibility in respect of data security;
- Introduction of data protection at the stage of planning when it processes personal data and makes impact assessment, when the processing is of high risk for the rights and freedoms of the data subjects;
- Integration of data protection in its internal documents;
- Provision of regular training for the staff in connection with the data protection matters, for example: rights of the data subjects, consent, legal basis, impact assessment and breach of the data protection. The organization shall keep a register for the attendance in respect of these trainings and on behalf of the staff.

- Regular testing of the measures for provision of protection and a periodical audit with the purpose to be assessed the efficiency and the level of observance.

13.2. Registers

According to the requirements of GDPR, AUBG shall keep complete and correct documentary records about it the activity that relates to the processing and keeping of correct and actual registers which shall give information about each processing, including a register of the received consents and procedures for the receiving of the consents.

These registers shall at least include the name and the contact information of the administrator and the data protection officer, clear description of the type of personal data, data subjects, processing operations, processing purposes, third parties, receivers of personal data, place of keeping personal data, transfers of personal data, specified time for keeping personal data and description of the protection measures.

13.3. TRAINING AND AUDIT

GDPR obliges each administrator to provide adequate training of its staff and which shall help for the compliance with the requirements of GDPR, as well as regular testing of the systems and processes connected with the processing.

13.4. Data protection at the stage of planning and impact assessment

AUBG is obliged to introduce measures for data protection at the stage of planning when personal data is processed and through the introduction of relevant technical and organizational measures. This includes consideration of the necessary level of data protection at the stage of planning for all programs/systems/processes, as the following has to be taken into consideration:

- The used technology;
- The connected with the introduction costs;
- The type, scope, context and purposes of processing, and
- The risks (of different probability and seriousness) about the rights freedoms of the subjects which arise out of processing.

The administrators shall also make impact assessment of high-risk activities which relate to processing, as well as to discuss the results with the data protection officer every time when a key system is introduced or a business program is replaced and which is connected with the processing of personal data, including:

- The initial introduction of new technologies or the transition to new technologies;
- Automated processing, including profiling or automated taking of a decision;
- Processing of sensitive personal data on a large scale;
- Large-scale and systematic monitoring of a public zone;
- The impact assessment shall include:

- Description of the processing, its purposes and the legitimate purposes of the administrator, if necessary;
- Assessment of the necessity and proportionality of processing in respect of its purpose;
- Risk assessment in respect of the persons and the taken measures for management of the risk;
- Automated processing (Including profiling) and automated taking of decisions.

In general, the automated taking of decisions is forbidden when the decision leads to legal consequences for the data subject, unless:

- The data subject has given his/her explicit consent;
- The processing is allowed by law, or;
- The processing is necessary for execution or conclusion of a contract.

If concrete types of sensitive personal data are processed, then reasons II.) and III.) are not applicable, as this sensitive personal data can be processed when this is necessary (unless other measures can be used where the same intrude the privacy of the person in a less degree) for the purposes of an important public interest and which for example is the fraud prevention.

If a specific decision is fully based on automated processing (including profiling), then the data subjects have to be informed about the right to object this processing at the time of the first communication with them. The attention of the subjects has to be only turned to this right that belongs to them.

AUBG also has to inform the subject about the logics that is used at the time of the taking of automated decisions of profiling, if such are applied, the importance and the possible consequences, as well as to give the subjects the right to require human intervention, to express their point of view or to dispute the decision;

The impact assessment shall be made every time when it is undertaken automated processing (including profiling) or automated taking of decisions.

13.6. Direct marketing

AUBG is subject to concrete rules and laws when marketing messages are sent to clients.

For example, the prior consent of the data subject is required for electronic direct marketing (via email, sms or automated calls). There is a limited exception to this rule in respect of existing data subjects which allows the organizations to send marketing messages if:

- they have received contact information over the course of a sale;
- the marketing message refers to similar products or services and there is a possibility for the person to refuse future messages, both at the time of the provision of personal data and at the time of any subsequent message.

The right of objection against the marketing messages has to be explicitly presented to the data subject, so that to be easily distinguished from the rest of the information.

The objection against the marketing messages shall be taken into consideration in due time.

13.7. Sharing of personal data

In general, AUBG is not allowed to share personal data with third parties, unless there are appropriate protections and contractual relationships.

Each employee can share personal data which he/she processes, as he/she can share it with another employee of AUBG if the execution of the official duties of the receiver requires access to the data.

Each employee can share personal data which he/she controls, as he/she can share it with third parties, such as subcontractors and if the following conditions are kept:

- They shall posses this information with the purpose to implement a service under a contract;
- The sharing of personal data is in compliance with a data protection statement which is provided to the subject and if it is necessary, the consent of the subject is given;
- The third party has agreed to observe the necessary data security standards, policy and procedures;
- The transfer is in compliance with the applicable limitations concerning the transfer to countries out of the European Economic Area, and
- There is a duly concluded contract for processing, where the same is concluded with the subcontractor who corresponds to the requirements of GDPR.

14. Changes of these internal rules

AUBG reserves the right to change these internal rules at any time and without a notice. Please, regularly check for the latest version of these rules.

These internal rules do not have priority over any applicable law.