

REGULATION

“ON THE PROTECTION, PROCESSING, PRESERVATION AND SECURITY OF PERSONAL DATA”

Adopted by Decision No. 30 dated 27.09.2018 of the Meeting of Judges

Amended by Decision No. 2, dated 14.01.2020 of the Meeting of Judges

Amended by Decision No. 86, dated 07.12.2022 of the Meeting of Judges

(updated version)

CHAPTER I GENERAL PROVISIONS

Article 1

Object

The object of this regulation is to set out organizational and technical procedures, measures for the protection of personal data, as well as security, preservation and administration of such data with the AC structures.

Article 2

Purpose

1. This regulation is designed for the purpose of establishing organizational and technical measures for protection, preservation, security and administration of personal data. It applies to all kinds of data processed by the AC under “Law on personal data protection”.
2. The processing of data is done in accordance with the Constitution, Law on protection of personal data, legislation governing the AC activity and with the principles guiding the re-evaluation and disciplinary jurisdictions, having due regard for human rights and fundamental freedoms.

Article 3

Legal basis

1. Domestic legislation:
 - a. Constitution of the Republic of Albania, Articles 15-58.
 - b. Law no. 84/2016 “On the transitional re-evaluation of judges and prosecutors in the Republic of Albania” (hereinafter, Law 84/2016).
 - c. Law no. 49/2012 “On administrative courts and adjudication of administrative disputes”
 - ç. Law no. 9887, dated 10.03.2008, “On Protection of Personal Data”, as amended.
 - d. Orders, Instructions and Decisions of the Commissioner for the Protection of Personal Data.
 - dh. Legal acts and organic by-laws on the organization and functioning of the Appeal Chamber.

2. Foreign legislation:
 - a. Universal Declaration of Human Rights;
 - b. Convention on the Protection of Human Rights and Fundamental Freedoms, amended by Protocol no. 11, entered into force on November 1, 1998¹;
 - c. Directives 2002/58/EC and 95/46/EC of European Council and European Parliament;
 - ç. Convention no. 108 “On the protection of individuals with regard to Automatic processing of personal data, ratified by Law no. 9288, dated 7.10.2004;
 - d. Addendum protocol of the Council of Europe Convention “Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and trans-border data flows”, ratified by Law no. 9287, dated 7.10.2004.
3. Should the personal data be classified as “state secret”, the legislation on the classified information “state secret” shall apply.

Article 4

Definitions

Amended by Decision No. 2, dated 14.01.2020 of the Meeting of Judges
Amended by Decision No. 86, dated 07.12.2022 of the Meeting of Judges

1. For the purposes of this Regulation, the following terms shall have the following meaning:
 - a) “**Personal data**” shall mean any information relating to an identified or identifiable natural person. Elements used to identify a person directly or indirectly, referring in particular identity numbers or other factors specific to his physical, psychological, economic, social and cultural identity.
 - b) “**Sensitive data**” shall mean any piece of information related to the natural person in referring to his racial or ethnic origin, political opinions, trade union membership, religious or philosophical beliefs, criminal prosecution, as well as data concerning his health and sexual life.
 - c) “**Processing of personal data**” shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, preservation, adaptation or alteration, retrieval, consultation, use, transmission, dissemination or otherwise disclosure, spread or combination, photographing, reflection, entry, completion, selection, blocking, erasure or destruction, even though they are not recorded in a database.
 - ç) “**Anonymization**” is the process of erasing personal data in the text of judicial decisions.

¹ Protocol no. 14, Law no. 9453, dated 15.12.2005

- d) **“Controller”**, for the purposes of this regulation, the Appeal Chamber, which determines the purposes and means of processing of personal data, in compliance with the laws and by-laws applicable, and it is responsible for the fulfillment of the obligations defined in law.
 - dh) **“Processor”**, for the purposes of this regulation, any natural or legal person, contracted for various activities and services, besides AC staff, which processes personal data on behalf of the latter, in accordance with the terms and liabilities set forth by AC.
 - e) **“Recipient”** shall mean any natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not.
 - ë) **“Subject of personal data”** shall mean any natural person whose personal data are processed during the re-evaluation, such as the subjects provided for in Articles 179/b, 179, paragraph 7, of the Constitution of the Republic of Albania, Article 17, paragraph 1 of Law 84/2016, AC judges, personnel, related persons, third persons, visitors and denouncers.
 - f) **“Judicial data”** shall mean any information related to AC decisions under the Re-evaluation and Disciplinary Jurisdictions, or to records in the AC registers, as determined by Article 16, paragraph 1, items ‘a’, ‘b’, ‘c’ and ‘ç’ of the Regulation “On the Activity of the Appeal Chamber of the Constitutional Court”, as well as any data provided for in Law no. 9887, dated 10.03.2008, “On the protection of personal data”, as amended
 - g) **“Archiving system”** is any structured group of personal data, accessible on the basis of specific criteria.
 - gj) **“Audio-video system”** is a CCTV system, which uses cameras, archiving devices and other auxiliary devices which store and process data.
2. The other terms used for the purpose of this Regulation shall have the same meaning as in Law no. 9887, dated 10.03.2008 “On the protection of personal data”, as amended.

Article 5

Scope

This regulation shall apply to the processing of personal data, fully or partially, by automatic or other means, kept in an archiving system, or intended to form part of the archiving system of the Appeal Chamber.

CHAPTER II

PROCESSING OF PERSONAL DATA

Article 6

Protection of personal data

1. The AC shall take appropriate organizational and technical measures to protect personal data from unlawful or accidental destruction, accidental loss, in order to protect access to or dissemination by unauthorized persons, in particular when data processing takes place in networks or any other illegal form of processing.
2. The instituted measures shall include, but not be limited to:
 - a) Processing of personal data and their transmission only in compliance with the scope and activity of the Appeal Chamber in the capacity of controller;
 - b) Compliance with the principle of lawful processing of personal data, with due regard for human rights and fundamental freedoms, and in particular, the right to protection of private life;
 - c) A fair and lawful processing;
 - ç) Collection of personal data for specific, clearly defined and legitimate purposes, and their processing in compliance with these purposes;
 - d) Adequacy of data, in accordance with and proportionate to the purpose of processing;
 - dh) Data should be accurate in terms of facts they depict, and where appropriate, they shall be updated or subject to any other action necessary to make sure that inaccurate and incomplete data are deleted or corrected;
 - e) Data should be kept in such a form as to allow the identification of the subjects they belong to for a certain period of time, but no longer than necessary for the purpose for which they were gathered or processed.

Article 7

Processing purpose

1. The purpose of processing of personal data for the assesseees, related persons to the assesseees, or other related persons to them, as well as subjects under the Disciplinary Jurisdiction, is the fulfilment of the obligations under the Constitution, Law no. 84/2016 “On the transitional re-evaluation of judges and prosecutors in the Republic of Albania” and Law no. 96/2016 “On the status of judges and prosecutors in the Republic of Albania”.
2. The purpose of processing the personal data of individuals who make submissions regarding assesseees under disciplinary or re-evaluation jurisdiction, is the identification of such individuals.
3. The purpose of processing the personal data of AC judges and staff members is due to their employment with the AC, and meeting the obligations on the administration of employee’s personal files.

4. The purpose of processing the personal data of visitors or media reporters is their identification to ensure the protection of staff, documentation, etc.

Article 8

Criteria of personal data processing

1. AC staff members handling personal data of the assessee shall comply with the criteria under Article 6 of Law “On the protection of personal data”.
2. Exceptional cases for personal data processing, relate to:
 - a) The assessee, for whom such rights and freedoms are restricted under Article A of the Annex to the Constitution;
 - b) information on public officials or public servants, which are subject to restrictions under Article 4, paragraph 4, item b, of Law “On the protection of personal data”.

Article 8/1

Data collection and processing

Added by Decision No. 86, dated 07.12.2022 of the Meeting of Judges

1. The collection and processing of personal data for the assessee and for the subjects within the Disciplinary Jurisdiction, shall be carried out in accordance with the purpose of Law no. 84/2016 “On the transitional re-evaluation of judges and prosecutors in the Republic of Albania”, to the purpose of their transitional re-evaluation and in view of the consideration of the request/appeal, according to the provisions of Article 5, paragraph 3 of Law no. 84/2016 “On the transitional re-evaluation of judges and prosecutors in the Republic of Albania”, and cannot be used for other purposes.
2. The collected data shall include information on the assessee, related persons and other related persons, as well as data on subjects within the framework of the Disciplinary Jurisdiction, according to the provisions of Law no. 84/2016 “On the transitional re-evaluation of judges and prosecutors in the Republic of Albania”.

Article 9

Processing of sensitive data

The sensitive data for all employee are processed in accordance with the criteria defined in Article 7 of Law “On the protection of personal data”, as amended.

Article 9/1

“Processing of the data using the audio-video system”

Added as per Decision No.2, dated 14.01.2020 of the Meeting of Judges

1. The Appeal Chamber processes “images, audio and video” data by means of an audio-video system installed in the courtroom premises, according to Article 6, paragraph 1, of Law no. 9887, dated 10.03.2008 “On personal data protection”, as amended. The main aim of the installation of the audio-video system is establishing an institutional archive to store the public hearings, as well as monitoring the public hearings for security purposes.
2. Processing of personal data by means of the audio-video system (CCTV) is not object of the Law no. 119/2014 “On the right to information”.
3. The courtroom is provided with the standard information board model on the monitoring through the surveillance system, approved by the Commissioner for the Right to Information and Protection of Personal Data, according to paragraph 5/iv of Instruction no. 03, dated 05.03.2010, “On processing of personal data in video surveillance system in facilities and other premises”.
4. The data stored by means of this system throughout the period this institution shall exercise its activity, shall be archived electronically in compliance with the legislation in force on achieve of electronic document, provided for in Article 18 of Law no. 10273, “On the electronic document”, as amended.

Article 9/2

CCTV data processing

Added by Decision No. 86, dated 07.12.2022 of the Meeting of Judges

1. The processing of personal data by means of the AC CCTV shall be carried out for the fulfillment of the tasks defined in Law no. 84/2016, “On the transitional re-evaluation of judges and prosecutors in the Republic of Albania”, for the security and protection of judges, international observers appointed by the International Monitoring Operation, advisory and administrative personnel, “State Secret” classified information and the institution’s property under administration.
2. The recordings of personal data through the CCTV may only be used for the investigation of an event that has brought about damage to the interests protected by law, according to the definition of paragraph 1 of this article.
3. Personal data processed through the AC CCTV system shall be stored for a period of up to 21 (twenty one) days and, following the elapsing of that period, the data shall be deleted.

4. The AC administers the daily registrations and shall be responsible for the protection of personal data.
5. Personal data processed through the CCTV shall be kept safe and their misuse or corruption in any way is prohibited. The IT specialist must take all technical and organizational measures to minimize the risk of their misuse or corruption.
6. The subjects of personal data are clearly informed that the CCTV is in operation in the internal and external premises of the institution, by placing written boards in monitored premises, according to the standard model of the information board adopted by the Commissioner for the Right to Information and Protection of Personal Data.
7. The transmission in real time via Internet or other similar services of images recorded through the CCTV, where people are easily identifiable, shall be prohibited.
8. It shall be forbidden to install the CCTV system in premises used exclusively for private purposes, such as, the dining area, toilets, etc.
9. Any person operating the CCTV system, under the authority of the controller, must not process the personal data to which he has access, without the authorization of the head of the institution, except when bound by law.
10. The responsible structure for the security of the AC premises (the Republic Guard), in the capacity of “Processor”, shall be bound to observe the provisions of paragraph 6 of this article, for the processing of personal data by means of the CCTV.

Article 10

International data transfer

1. Every AC employee shall apply the provisions of Articles 8 and 9 of Law “On the protection of personal data” and related by-laws in the case of international data transfers.
2. Data and information may be communicated to counterpart institutions in foreign countries based on cooperation agreements, provided that the requesting country handles and keeps such data in accordance with the data protection legislation.
3. Data and information transferred under the above paragraph shall be handled only by the relevant authorities of the recipient country.
4. International data transfer for purposes of the re-evaluation process shall be conducted in accordance with Article A of the Annex to the Constitution and Article 50, paragraph 7, of Law 84/2016.
5. “Top secret” data shall not be transferred through electronic communication channels.

6. “Secret” data may be transferred through electronic communication channels in encrypted form. Encryption shall be handled by the units responsible for data protection. This means that the procedures and measures of encryption for data transfer shall be determined by the AC.
7. The AC shall abide by and institute measures for the encryption of data transfer in accordance with the applicable legislation on state secret.

CHAPTER III THE RIGHTS OF THE SUBJECTS OF PERSONAL DATA

Article 11

Compliance with individual rights

1. Dissemination or communication of personal data is conducted in accordance with the purpose for which such data are gathered.
2. Through a written request, every individual may have access to his personal data as processed by the AC, except for data related to the re-evaluation process.
3. Pursuant to Law no. 9887, dated 10.03.2008 “On protection of personal data”, as amended, the AC is obliged to observe the following rights of the subjects of personal data:
 - a. the right to access;
 - b. the right to request their blockage, correction or deletion;
 - c. automatic decision-making;
 - ç. the right to challenge;
 - d. the right to appeal;
 - dh. the right to indemnification.
4. The written request should contain sufficient data to establish the identity of the requester. Within 30 days from the receipt of the request, the controller shall duly inform the requester/requesting individual or explain to him/her the reasons for withholding the information.

Article 12

Requests for information

1. Provided the re-evaluation process is not impaired, under Article 4, paragraph 7 of Law 84/2016, requests for information may be submitted by:
 - a. The assessee himself/herself;
 - b. The duly authorized legal representative;
 - c. Persons related to the assessee, as defined by Article 3, paragraph 13, of Law 84/2016, in connection with personal data related to them;
 - ç. Other individuals, without a direct stake, demonstrating a lawful interest in such data, whose

interest is in line with the purpose such data are gathered for. Such access shall only be restricted for purposes related to the re-evaluation process.

- d. The parent or caretaker, if:
 - i. the child does not have the capacity to act;
 - ii. the parent is acting in the child's interest.
2. In each case, a response is sent to the address indicated by the requester.

CHAPTER IV PERSONAL DATA PROCESSING IN AC DECISIONS

Article 13

Personal data in decisions

1. At the conclusion of the case review, the AC pronounces the final decision.
2. "Personal data" in AC decision have the same meaning as the one mentioned in Article 4 of this Regulation.
3. Prior to the publication of the final decision on the AC website, the process of anonymization of personal data shall be conducted whenever:
 - a) they relate to the identities of the parties, third persons, witnesses and experts summoned by the court;
 - b) they impair the privacy of parties to the case (such as: address, license plate, telephone numbers and any other element that may identify the holder of personal data);
 - c) they regard the identities of parties/shareholders, number of shares/quotas owned by the parties, bank accounts, currency amounts and commercial secrets;
 - ç) they involve third persons who may, even indirectly, disclose the identity of minors, whenever they are involved by the decision;
 - d) any other data that may impair the dignity and privacy of parties or persons related to the judicial case.

Article 14

Anonymization and publication of decision

1. Every personal information in the meaning of Article 3 of Law no. 9887, dated 10.03.2008, "On the protection of personal data", as amended, in the text of the judicial decision is encrypted and replaced by the symbol: {***}.
2. Under the supervision of the legal adviser, the judicial secretary carries out the anonymization of the personal data in the decision text.
3. If it appears that personal data in the unpublished court decision are inaccurate or incomplete, the legal adviser shall consult with the case rapporteur/chair on their correction or deletion.

Following this consultation, correction, deletion blockage is carried out in accordance with the law on personal data protection.

4. The text of the judicial decision, which has been encrypted as described in paragraph 1 of this Article, is published on the AC official website, under “Decisions”.
5. The judicial secretary enters into the inventory of the case file the original decision signed by the adjudication panel and the anonymized decision published on the AC official website.

Article 15

Right to access to anonymized decisions

1. The Appeal Chamber shall publish only the anonymized text of the decision.
2. The text of the decision with the complete personal data is available only to the AC staff on the Case Management System.
3. The AC ICT Specialist shall create passwords for AC inner users (judges and AC staff members) to enable access to decisions containing complete personal data.
4. A copy of anonymized decisions is made available to interested persons for scientific, statistical, literary or journalistic use, in accordance with the applicable legal provisions.
5. A copy of the decision, with the full personal data, is made available to the assessee or his/her legal representative, as well as to the institutions with a legitimate interest in the re-evaluation process.

CHAPTER V

SECURITY OF PERSONAL DATA

Article 16

Measures for data security

1. The AC shall take appropriate organizational and technical measures to protect personal data from unlawful or accidental destruction, accidental loss, in order to protect access to or dissemination by unauthorized persons, in particular when data processing takes place in networks or any other illegal form of processing under Article 27 of Law no. 9887, dated 10.03.2008, “On the protection of personal data”, as amended.
2. The protection of personal data is carried out through taking the organizational measures, which consist of:
 - a) Defining of organic functions for the use of personal data
 - b) Access to personal data and electronic systems which process these data, only by the authorized persons through authentication process.
 - c) The authorized person for the processing of data stored in the audio-video system is the IT Specialist, who is certified at ‘Top Secret’ level, issued by the Directorate of Securing Classified Information
3. The protection of personal data, in addition to other measures, is also carried out through the

following safety precautions:

- a) installing and automatic updating of an antivirus system and double firewall system, which is managed via the servers and network equipment.
- b) updating the operational and renovation system of computer software.
- c) granting access to staff to only those materials necessary for completing their tasks;
- ç) using passwords;
- d) setting up a backup system.
- dh) keeping track of every action on personal data, both in hard copy and electronic form.

Article 16/1

“Measures for the security of the audio-video data”

Added by Decision No. 2, dated 14.01.2020 of the Meeting of Judges

1. The AC audio video electronic system shall be used only for carrying out the scope defined in this regulation. This system is used by the IT Specialist. In case of need for maintenance purpose or repair, the system shall be accessed even by third specialized persons, under the supervision of institution’s personnel.
2. IT specialist registers and document by means of a record for every necessary modification in case of any mistake, defect or incident in the audio-video system.
3. For every case foreseen in paragraph 2 of this article, the IT Specialist shall notify immediately his/her director, who in turn informs the Secretary General and president of the institution, and conduct the relevant repair after having their authorization.
4. The use of the system is carried out by the IT Specialist in line with the duties defined in the job description, pursuant to the regulation “On the organization and functioning of personnel and administration of documentation”.
5. Whenever the IT specialist responsible for the use of audio-video system changes or leaves his job position, he/she shall loss the right to have access related to the previous duty.

Article 17

Actual security measures to secure the premises

Added and amended by Decision No. 86, dated 07.12.2022 of the Meeting of Judges

1. Premises where personal data are processed must be protected through organizational, physical and technical measures designed to prevent access of unauthorized persons to the premises and equipment used in personal data processing.
2. Security measures shall be applied commensurate with the level of security of the administered data and information, and the risk rate indicators from unauthorized exposure of stored information.
3. Security measures of premises where personal data are processed shall include, but not be limited to, the following:
 - a) Prohibition of unauthorized individuals in the AC premises.

- b) 24-hour surveillance of AC entrance.
 - c) Alarm system, video-cameras, etc., shall be installed, in addition to other security measures;
 - ç) Checks shall be run to prevent the installation or use of interception and audio recording devices.
 - d) The premises shall be guarded continuously by the Guard of the Republic.
4. Other additional measures are also used for the security of the premises, provided for in the legislation for the “State Secret” classified information, due to the AC mission and activity.

Article 18

The following individuals are allowed to stay in the premises where personal data are processed:

1. AC staff members, whenever this is essential to the completion of their tasks.
2. System or telecommunication maintenance staff are allowed to enter such premises in the company of the staff member designated by the head of the institution whenever necessary.

Article 19

Duplication of data

1. The ICT Specialist must have a copy and a duplicate of all data and software stored or installed in the main computer. The duplicate copy must be kept in a safe place which meets the technical conditions of information storage.
2. The number and form of additional copies of documents and other communication devices through which they are stored, are determined by the department responsible for each document.

Article 20

Protection of electronic equipment

Electronic equipment for data and information processing at the AC must be used solely for completing the tasks in the regulation. These equipment shall be used by only AC staff trained to use them. The training of the AC staff dealing with automatic processing of data is done by a software supplier or the ICT Specialist. For every error or malfunction in the AC systems the system administrator is notified, who proceeds to redress the problem based on request.

Article 21

Protection of software programs

1. The Directorate of Case Management and Relations with the Media and Public is responsible for managing programs dealing with data and information processing, whether purchased or donated. In the case a staff member not primarily involved in software development and planning, develops a data processing program, before such program is mainstreamed in the operations, the ICT specialist must review and approve it. Following approval, the ICT specialist arranges for its installation in each electronic equipment.
2. Upon orders from the direct superior, for each program, the ICT specialist shall decide:
 - a) The person entitled to delete, copy or modify it;
 - b) The location the copy will be kept and the person responsible to its update.

Article 22

Programs purchased by AC, must be provided with the licenses to allow the AC to install and use them.

Article 23

Passwords

1. Many of the computer applications and systems are protected by passwords. For security purposes, these passwords must be changed (*every three months*). Some rules on the use and creation of passwords are:
 - a. They must not be shared with other persons inside or outside the institution (*for example, passwords to personal computers*). Staff members are responsible for protection and non-dissemination of this information.
 - b. They must be easily remembered words or phrases; however they must not be readily identifiable, for example, names or addresses. It is advisable to use strong passwords which are those that contain upper and lower case letters, numbers and symbols.

Article 24

Monitoring and recording access to personal data

1. Access to data and information is subject to special security measures to guarantee their inviolability and constant updating. The system should be constructed in such a way as to ascertain the identity of the user. This requires that the central server should recognize every terminal operator and every user through special programs. This system must enable the constant identification of users at any time, at any given terminal, workplace, or other devices over the period for which specific data will be stored.
2. Users have the right to information on the kind of data related to daily registrations and the

timeframe of preservation of such registrations.

3. Daily registrations are administered by the ICT Specialist who is responsible for data protection and determines the content of daily registration and the timespan for preservation of personal data. The period of preservation of data registration should be the same as the period of preservation of hard copies containing such data. Upon expiry of this timeline the data are either archived or eliminated. Identification and registration of terminal operators and users is done through passwords for entry into the database. Passwords are secret and personal.
4. Access to data is allowed or prohibited by special electronic applications/software. Control and recording of access to such data and information is handled by responsible persons for data protection.

Article 25

Protection of documents

Classified documents and other communication means in which personal data are recorded must be specially encrypted. Their level of classification should be marked based on Law no.8457, dated 11.2.1999 "*On classified information "state secret"*", as amended. Encryption and level of classification must be in accordance with the applicable legal provisions.

Article 26

Secret documents

1. Whenever documents containing data considered "top secret" or "secret" are created, data related to number of copies (written, printed, designed, duplicated) and name of the recipient is accordingly recorded on the original copy. If reproduction is allowed, every copy should have its registration number in the reproduction register.
2. If the material mentioned in the above paragraph is made up of several pages or is attached to other documents, or has other constituent parts, every page must be secured with a certain confidentiality level or measures must be taken that its pages or attachments be not removed or destroyed without prior warning.
3. In case confidential information is presented on a screen or other display systems, the level of secrecy or confidentiality must be indicated in every part (illustrations, pictures, observations, projections, etc.).

Article 27

Preservation of secret documents

1. Documents containing “top secret” or “secret” information must be preserved in accordance with the applicable legislation on information classified as “state secret”, as well as on the AC regulation “On the organization and functioning of AC staff and administration of AC documentation”.
2. The places where documents mentioned in the above paragraph are kept will be accessed only by employees creating, using, protecting or securing these documents.

Article 28

Destruction, elimination of draft versions of “state secret”classified documents

1. Draft materials used to create documents containing “top secret” or “secret” information (matrixes, calculations, diagrams, schemata, and discarded prints) must be eliminated. The manner of their elimination must be one that renders them illegible in order to prevent any reproduction of content.
2. The commission created for destruction/elimination of material keeps minutes on their destruction, based on the paragraph above, which minutes are subsequently signed by the members of the commission. The commission must be composed of three members assigned by the head of relevant unit. The procedure to be used for destruction of documents containing personal data is determined by the head of respective unit.
3. The same procedure shall also be used for destruction of data, documents and communication tools whose preservation time has expired.

Article 29

Program duplicates

Duplicates of programs with data to be used in the event of natural disasters or extraordinary situations or warfare, must be kept in places or locations outside the main office of the relevant organizational unit. The manner of creation, multiplication and maintenance of these duplicates must be determined specifically for each document in accordance with the rules of their preservation and security. These rules shall be determined by the relevant organizational unit, in accordance with the rules applicable to natural disasters.

Article 30

If a document containing confidential information is lost or disappears, the competent employee has the duty to immediately inform his/her superior and take any measures deemed necessary to identify the circumstances of the loss or disappearance and to eliminate the negative consequences.

CHAPTER VI
ADMINISTRATIVE SANCTIONS

Article 31

Administrative measures

Every AC employee who fails to protect personal data shall be held responsible for violation of discipline, rules and obligations of his position. If his/her actions do not constitute a criminal offence, he/she shall be subject to administrative and disciplinary measures as prescribed by the relevant legislation.

Article 32

Supervision of protection measures and procedures

The implementation of rules for the protection of personal data, enforcement of security measures, and safety of automated data, against accidental destruction, as well as against their unauthorized modification and dissemination, is the responsibility of individuals charged with the supervision and protection of respective data.

CHAPTER VII
FINAL PROVISIONS

Article 33

Confidentiality of data processing

1. Every AC employee processing personal data or receiving knowledge of processed data may not disclose their content to other persons. He/she is obliged to protect their confidentiality and trustworthiness even following leave from office.
2. Every AC employee with access to personal data has the obligation to sign a declaration of confidentiality which is administered by the AC.
3. Every person under the controller's authority must not process personal data which are accessible to him without the controller's authorization, unless obliged by law.

Article 34

Timeframe of data protection

1. Personal data of AC staff shall be preserved in accordance with the timeframes fixed in legislation on the archives. Data submitted in job applications shall be preserved for a period of six months from the day of their lodging with the institution.

2. Personal data of the public members who make submissions on assesseees shall be preserved over periods valid for the case file under which they belong.
3. Personal data of AC visitors shall be preserved for a period of two months.

Article 34/1

Contact Person for Data Protection

Added by Decision No. 86, dated 07.12.2022 of the Meeting of Judges

1. The Contact Person for Data Protection (hereinafter “CPDP”) is the person appointed by order of the head of the institution, according to the provisions of Chapter VI of Instruction no. 47, dated 14.09.2018, of the Commissioner for the Right to Information and Protection of Personal Data “On the rules for maintaining the security of personal data, processed by large processing entities”.
2. The CPDP, in addition to his functional task, exercises, but is not limited to, the following tasks and responsibilities:
 - a) Conducts internal supervision of the fulfillment of obligations for the protection of personal data by the subject processing personal data, in accordance with the provisions of this regulation.
 - b) Responds to the implementation of technical and organizational measures, also in relation to personnel, in accordance with the provisions of this regulation, and supervises as well their practical implementation.
 - c) Responds for the internal supervision of the activity of the processor, for the content and drafting of the written contract, in case of contracting a processor by the subject processing the personal data. During the duration of the contractual relationship or authorization, the contact person shall verify the compliance with the approved terms, including the commitment and change of processors, if any.
 - ç) Responds for the internal supervision of international transfers of personal data, in accordance with the provisions of this regulation.
 - d) Responds for the submission of archiving systems documentation for special registration and announcement of changes and deregistration of archivation systems from the special register. Maintains records of archiving systems that are not subject to registration and makes them available to anyone legally entitled to their access.
 - e) Presents the written authorization, at the request of the Commissioner, on the basis of which he acts, as well as evidence of the level of knowledge acquired in professional training.
3. The CPDP reports directly to the highest management level of the controller.
4. The CPDP is the AC contact person with the Office of the Commissioner for the Right to Information and Protection of Personal Data.
5. The CPDP shall cooperate with the Coordinator for the Right to Information in handling requests, with the aim of balancing the right to information with the protection of privacy.

6. The CPDP shall cooperate with the AC structures to meet all legal obligations in accordance with the legislation for the protection of personal data.
7. The CPDP shall inform the AC staff about the legal obligations on a case-by-case basis related to developments in the field of personal data protection

Article 35

Sanctions

Failure to comply with the requirements of this regulation shall constitute violation of work discipline and shall be punishable in accordance with the applicable legislation and AC regulations.