

1. GENERAL PROVISIONS

1.1. This provision on the video surveillance policy (hereinafter referred to as the Policy) determines the procedure for using video equipment and organizing a video surveillance system (direct implementation of video surveillance through the use of video cameras to obtain video information about the facility and premises, as well as recording the resulting image and storing it for subsequent use) in the premises GNC-ALFA CJSC (hereafter referred to as the Company) and is designed to inform clients and employees visiting the viewing areas of surveillance cameras installed at the Company's facilities about the purposes of processing their images.

1.2. The Policy has been developed in accordance with the law of the Republic of Armenia dated 18.05.2015 No. ՀՕ-49-Ն "On the Personal Data Protection" (hereafter referred to as the Law), Policy on Information Security and the Personal Data Processing of the Company, other regulatory legal acts of the Republic of Armenia.

1.3. The video surveillance system is an element of the Company's overall security system, aimed at ensuring public safety, preventing possible unlawful acts against visitors, employees and clients of the Company, as well as the Company's property, preventing emergencies and (or) incidents, ensuring the objectivity of the investigation in cases of their occurrence (hereinafter referred to as non-standard situations).

1.4. The Policy is published in the public domain on the Internet on the Company's official website at <https://ovio.am>, and is also publicly accessible in the administrative area (reception).

2. PRINCIPLES OF VIDEO SURVEILLANCE AND VIDEO RECORDING

2.1. The surveillance system and video recording system are based on the principles of legality, proportionality, transparency, integrity and security.

2.1.1 **Principle of legality** – The Company organizes video surveillance in compliance with the requirements of the law, for legal and specific purposes and cannot be used for other purposes.

2.1.2 **Principle of proportionality** – The Company uses video surveillance in cases where it is impossible to achieve established goals without it. The Company ensures a balance between the pursued purpose of video surveillance and protecting the privacy of people who are caught in the frame. Video recordings are processed to the minimum extent that is sufficient to achieve legitimate purposes. Whenever possible, cameras are installed so that objects relevant to the purposes of video surveillance are included in the frame.

2.1.3 **Principle of transparency and integrity** – The Company informs personal data subjects about the implementation of video surveillance by placing warning signs on the entrance door to the Company's office premises. The Company prohibits the use of devices intended for secretly obtaining information. The Company, based on the criticality of the protected facility, may not indicate the location of the cameras.

2.1.4 **Principle of security** – The Company processes data in a manner that ensures adequate security of personal data, including protection against unauthorized or illegal processing, as well as against accidental loss, destruction or damage, using appropriate legal, organizational and technical measures.

2.2. You can familiarize yourself with other issues related to the personal data protection at GNC-ALFA CJSC, including information about the rights associated with the personal data processing, as well as the mechanism for their implementation, within the framework of the "Personal Data Processing Policy".

3. GOALS AND OBJECTIVES OF THE VIDEO SURVEILLANCE SYSTEM

3.1. The video surveillance system is an element of the Company's overall security system, aimed at ensuring public safety, preventing possible unlawful acts against the Company's employees, clients and Company's property, preventing emergencies and (or) incidents and ensuring the objectivity of the investigation in cases of their occurrence.

3.2. Video surveillance in the Company cannot be aimed at collecting information about a specific personal data subject.

3.3. The Company carries out video surveillance in all its buildings and premises.

3.4. The video surveillance system performs the following tasks:

3.4.1 ensuring the personal safety of the Company's employees and visitors;

3.4.2 safety of property, valuables and information of limited distribution of the Company;

3.4.3 strengthening the security of the Company's facilities;

3.4.4 prompt response to illegal actions in relation to property, valuables, restricted information, employees and visitors of the Company, as well as in the event of emergencies occurring at the Company's facilities;

3.4.5 ensuring measures for the safe operation of company facilities and self-service devices;

3.4.6 documenting incidents, emergencies and offenses at the Company's facilities, in places where self-service devices are installed and in the territory adjacent to the Company's facilities;

3.4.7 increasing the efficiency of actions in the event of non-standard situations, ensuring the objectivity of their consideration and assessment;

3.4.8 suppression of illegal actions on the part of visitors, employees and clients of the Company;

3.5. Video surveillance cannot be used for:

3.5.1 accounting of working time actually worked by the Company's employees;

3.5.2 unique identification of persons depicted in the video;

3.5.3 sound recording

4. PROCEDURE FOR ORGANIZING THE VIDEO SURVEILLANCE SYSTEM

4.1. Installation of the video surveillance system at the Company's facilities is carried out in accordance with its goals and objectives. The locations of video cameras and their technical characteristics are determined in accordance with specific tasks, based on the requirements of the instructions and other technical regulatory documents of the Company.

4.2. The Company's video surveillance system includes a number of devices: video recorders, video cameras, video monitors, etc.

4.3. Video surveillance is carried out around the clock and continuously using open video surveillance cameras. Cameras are installed based on architectural features with the condition that the camera lens must cover the entire room.

4.4. Surveillance cameras are installed in the following open areas:

4.4.1 on the Company's buildings to ensure perimeter security

4.4.2 a hall with video surveillance direction from the entrance to the office premises and towards the entrance to the office premises;

4.4.3 corridors with video surveillance on both sides of the corridor

4.4.4 to the office premises and with video surveillance directed to the emergency exit;

4.4.5 internal corridor with video surveillance direction to the warehouse;

4.4.6 open office premises ("open space" format) using additional technical means to ensure blurring of images of workplaces in order to prevent the receipt or dissemination of information constituting personal data, trade secrets, etc.;

4.4.7 premises for performances;

4.5. Surveillance cameras are installed in places that are not publicly accessible in the following areas:

4.5.1 in server rooms,

4.5.2 in critical network nodes (NODE),

4.5.3 warehouses,

4.5.4 other closed and restricted access areas.

4.6. Unlike open areas, for closed areas the Company may not indicate the location of the cameras, and they may not be visible.

4.7. It is prohibited to use devices designed to identify locations of invisible cameras on company premises.

4.8. Installation of video cameras in premises where the Company's employees do not perform official duties (restrooms, utility rooms, etc.) is prohibited.

4.9. The functions of ensuring the uninterrupted operation of video surveillance systems, carrying out regular technical monitoring and preventive maintenance, repairs, modernization and expansion of systems are carried out by authorized employees, with the involvement of third-party organizations that have the appropriate special permits (licenses) for the right to carry out security activities in terms of technical maintenance of equipment and security systems.

4.10. Unauthorized access to video camera settings, video recording modes and control of system peripheral devices is prohibited by any persons, with the exception of authorized employees and employees of organizations (legal entities) performing maintenance work on video surveillance systems of the Company's facilities.

4.11. Functions for ensuring storage security, setting up and changing system parameters, configuring the system, managing archiving parameters, managing access accounts to the video surveillance system (logins/passwords) and assigning access rights are carried out in accordance with the Information Security Policy and other local acts of the Company.

4.12. If information is received about the possible recording by video surveillance cameras of a situation that has signs of a disciplinary offense, an administrative offense, a criminal offense, on an oral instruction from the CEO of the Company (the person performing their duties), the Security Service and/or information security manager or the person responsible for internal control over the processing of personal data, for such video recordings the storage period may be extended for the period of relevant activities.

5. PROCEDURE FOR ACCESS TO VIDEO SURVEILLANCE SYSTEM RECORDINGS, STORAGE AND DESTRUCTION PERIODS FOR VIDEO SURVEILLANCE SYSTEM RECORDINGS

5.1. Access to recordings of video surveillance systems located at the Company's facilities is regulated by the Information Security Policy and other local acts of the Company.

5.2. Transferring access rights to video surveillance system recordings by users to other persons is prohibited.

5.3. Recording (copying) of video information from video surveillance systems of the Company's facilities to an external medium is carried out only by an authorized employee, on behalf of the CEO of the Company (the person performing their duties), the Security Service and/or the information security manager.

5.4. The storage period for video archives is set in accordance with the requirements of current legislation. The video surveillance system recordings information onto the hard drive of the video recorder. The storage period for the video archive is up to 90 days, depending on the location of installation and categories of the Company's premises, after which it is automatically deleted. In case of receiving information about the possible recording by video surveillance cameras of situations that have signs of committing a disciplinary offense, an administrative offense, or a criminal offense, the storage period for such video recordings may be extended, on the basis of clause 4.12, for the period of carrying out the relevant events provided for by the legislation of the Republic of Armenia. Also, the storage period for the video recording may be extended in the case of consideration of the client's appeal for the period of consideration of the specified appeal and resolution of the controversial situation.

5.5. Video recordings cannot be used by employees for personal or other purposes not related to professional activities, and are not subject to modification, use, distribution or provision, except in cases provided for by legislative acts.

5.6. The person responsible for the reasons for violating the confidentiality of video surveillance system recordings shall bear responsibility in the manner prescribed by the current legislation of the Republic of Armenia. The use of surveillance recordings for personal purposes is prohibited.

6. PROCEDURE FOR TRANSFERRING VIDEO SURVEILLANCE SYSTEM RECORDINGS TO THIRD PARTIES, EXERCISE OF RIGHTS RELATED TO THE PERSONAL DATA PROCESSING

6.1. Recording of video surveillance information is information of limited distribution and is not subject to transfer to third parties except in cases provided for by the current legislation of the Republic of Armenia.

6.2. Information obtained through video surveillance is provided to the relevant services and government bodies only upon their written requests in cases provided for by the current legislation of the Republic of Armenia.

6.3. In case of non-standard situations, viewing a copy of the video recording by the personal data subject is possible at the Company's office, provided that this copy of the video recording does not contain images of other personal data subjects. When a client contacts the Company with a request to view archived recordings of video surveillance systems, the Company's employee who communicates with the client identifies them, then generates and sends (via Microsoft Outlook) to the Security Service and the information security manager a request indicating the above information. If the request is approved by the above structural divisions, the authorized employee uploads the

requested archival video material and provides it to the initiator (the Company's employee) for demonstration to the client.

6.4. For assistance in exercising the rights related to the personal data processing in the Company, the personal data subject can also contact the person responsible for internal control over the personal data processing of GNC-ALFA CJSC by sending an email to pdpo@ovio.am.

7.FINAL PROVISIONS

7.1. This Policy comes into force from the moment of approval.

7.2. The Company has the right to use surveillance recordings as evidence in civil, criminal, and administrative proceedings to confirm the fact(s) of an unlawful act, as well as to establish other circumstances to be proven.

7.3. The Company has the right, at its own discretion, to unilaterally change and (or) supplement the terms of this Policy without prior notice to personal data subjects by posting a new version of the Policy on the Website.

7.4. Issues related to the personal data processing not addressed in this Policy are regulated by the legislation of the Republic of Armenia and the policy regarding the personal data processing.

7.5. If any provision of the Policy is found to be contrary to the legislation of the Republic of Armenia, the remaining provisions corresponding to the legislation of the Republic of Armenia remain in force and are valid, and any invalid provision will be considered deleted (modified) to the extent necessary to ensure its compliance with the legislation of the Republic of Armenia.