ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Μετανάστευσης & Ασύλου

@EDMIS IRIDA
6684f301972ec454ab5e8800
Ref. No: Υ.Σ.4498
Signature: 03/07/24 10:15
Distribution: 03/07/2024 10:17

Centaur Privacy Policy – Video Surveillance & Security Camera System in the MMA's Accommodation Facilities

1. **Purpose and scope of application of the video surveillance policy**

For the safety and security of the residents in the MMA's Accommodation Facilities, the staff and visitors, buildings and assets, the Ministry of Migration and Asylum (MMA) operates a video surveillance system. This policy describes the Ministry's video surveillance system and the safeguards taken by the Ministry, as an organisation for the protection of the personal data, privacy and other fundamental rights and legitimate interests **of persons** recorded on cameras.

The detection, investigation and criminal prosecution of criminal offences, as well as the protection of property assets and persons through the collection of personal data using video surveillance systems within the premises of the MMA's Accommodation Facilities. The MMA is constantly ensuring the appropriate 'safeguarding' tools, such as codes of conduct, certifications and marks, standard DPIAs, standard contracts

2. How do we ensure that the video surveillance system has been designed for the purpose of protecting privacy and data and is compliant with the data protection law?

2.1. **Compliance regime**. The MMA processes the images taking into account guideline 1/2011 of the Hellenic DPA and Guidelines 3/2019 of the European Data Protection Board [EDPB] [https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_el.pdf hyperlink to guidelines on the website of the European Data Protection Supervisor]. The process of compliance with Law 4624/2019 (Gov. Gaz. 137, Vol. A) is in progress, in adaptation and harmonisation with the General Data Protection Regulation (EU 2016/679, and Directive (EU 2016/680) of the European Parliament, which strengthens the framework for the protection of data subjects with regard to the processing of personal data in the European Union.

2.2. **Inspection by the Ministry.** The system is periodically audited – inspected for regulatory compliance needs by the internal services (Directorate General of Information Technology and Applications and the DPO) of the MMA itself.

2.3. **Notification of the compliance regime.** Pursuant to the Regulation, there is no obligation to notify and receive approval by the Hellenic Data Protection Authority for the installation and operation of a video surveillance system. The DPIA as updated and completed is a single and integral part of this Policy.

2.4. **Contacts with the competent data protection authority in the Member State**. The competent data protection authority will have at its disposal any information requested for the use of the system under the responsibility of the Data Protection Officer, who will keep a copy of the Processing File, a copy of the Security Policy and a Processing Risk Report.

2.5. **Decision of the Administration on the lawfulness of the video surveillance of the Accommodation Facilities.** The decision to use the current video surveillance system and to adopt the safeguards, as set out in this surveillance policy, was made by the competent Secretary General of the Department.

The main or general legal basis for the processing of the video surveillance is the performance of a task carried out in the public interest in the exercise of official authority (Art. 6 (1)(e) GDPR] while the processing of special categories of (biometric) data takes place for reasons of substantial public interest (Article 9 (2)(g) GDPR), under the Dublin III Regulation or the Immigration Code, while the Closed Controlled Access Centres (CCAC) constitute 'critical infrastructures of the State'. Pursuant to Article 6 (1)(e) GDPR, on the one hand, a legal basis for the processing of personal data is introduced without the need to be repeated in law, and, on the other hand, the processing, as a restriction to an individual right, should have a basis in the law of the Member State, in the sense that no specific provision of law is required for each individual processing operation (see Recital 45 GDPR), but the law must (see Recital 41 GDPR) expressly entrust to the controller the exercise of an official authority or the performance of a task carried out in the public interest in the course of which the processing is carried out as necessary for the fulfilment of the purposes of Article 6 (1)(e) GDPR (see HDPA Opinion 6/2016). The basis in national legislation is the existing legislation on immigration policy, which applies in conjunction with the new provisions of the GDPR and Law 4624/2019, Guideline 1/2011 HDPA on the protection of persons and goods, and Guidelines 3/2019 of the European Data Protection Board on the processing of personal data through video recording devices. Guideline 1/2011 stipulates (Article 2(1)) that the purposes for which personal data may be processed are the protection of persons and/or goods and the provision of health services. In the Greek legal order, the processing of personal data by a public authority is subject to Article 14 of Law 3917/2011.

In addition, there is an interconnection between the Centaur system and the Greek Police and therefore the possibility of processing special categories of data for law enforcement purposes cannot in principle be excluded. National legislation requires the controller to cooperate with law enforcement authorities (e.g. during an investigation), the legal basis for the handover of data is the legal obligation under Article 6(1)(c).

2.6. **Transparency.** The video surveillance policy has two forms, one for restricted use and one for public use, which are published respectively on the Intranet of the MMA and the MMA website. This public version of the video surveillance policy contains summary information on specific topics or attached documents. Information is only omitted from the public version when it is strictly necessary to maintain confidentiality for compelling reasons (e.g. for security reasons or to preserve confidentiality).

2.7. **Balance of interests:** It is mandatory to balance the interests. Fundamental rights and freedoms, on the one hand, and the legitimate interests of the controller, on the other hand,

should be carefully assessed and balanced. The processing is necessary for the purposes of the legitimate interests pursued by the controller, namely the safeguarding of property and the protection of residents, employees and other persons (due diligence obligations) on the premises of the accommodation facilities of the MMA, which are not overridden by the interests or fundamental rights and freedoms of the data subject that require the protection of personal data. The MMA may carry out video surveillance of persons staying in the accommodation facilities of the MMA, as there is a compelling legitimate interest that overrides the interests, rights and freedoms of the data subjects or for the establishment, exercise or defence of legal claims. The MMA applies the principle of proportionality to video surveillance systems: They must be appropriate and necessary in relation to the objective pursued, which cannot be achieved by less intrusive means.

They also have the right of access to data concerning them, as well as the right to request the rectification of inaccurate data or the erasure of unlawfully processed data (in the case of persons who have acquired the nationality of an EU Member State within the period of time elapsed since the submission of the application for international protection), and the right to be informed of the procedures for exercising these rights (see Article 29 of Regulation (EU) 603/2013).

The rights are exercised before the controller, which is the MMA.

The MMA assures that surveillance of residents in the accommodation facilities of the MMA is not allowed except in special exceptional cases:

– it is justified by the nature and living conditions in the accommodation facilities; and

– it is necessary to protect their health and safety or to protect critical areas within the accommodation facilities.

The Data collected through the video surveillance system will not be used as criteria for profiling or for evaluating their general behaviour (religious, racial, sexual, etc.).

The MMA assures that the surveillance of employees (public servants of the Reception and Identification Service and the Asylum Service of the MMA, police officers of the Ministry of Citizen Protection, employees of various specialties in Non-Governmental Organisations (lawyers, interpreters, social workers, psychologists, doctors, health professionals), staff of the European Asylum Support Office (EASO) and those recruited by the relevant Local Government Organisations through community service programmes provided by the Manpower Employment Organisation (OAED)) in workplaces is not allowed except in special exceptional cases:

– it is justified by the nature and conditions of work; and

– it is necessary to protect the health and safety of workers or to protect critical workplaces.

Data collected through the video surveillance system will not be used as exclusive criteria for evaluating employee behaviour and performance.

2.8. **Periodic reviews.** A periodic review of data protection will be carried out by Ministry officials annually. During the periodic reviews we will re-evaluate that:

- there is still a need for the video surveillance system;
- the system is still serving its stated purpose;
- the security measures of the recorded information are adequate;
- appropriate alternative solutions remain unavailable.

The periodic reviews will also cover all the other issues addressed in the first report, in particular whether our video surveillance policy continues to comply with the regulation and guidelines (adequacy check), and whether it is being followed in practice (compliance check). Copies of the periodic reports will also be attached to this video surveillance policy and will form a single and integral part of it.

2.9. **Privacy-friendly technological solutions.** The following technological and organisational solutions for privacy protection are also indicatively implemented (see guidelines, section 3.4):

- Special CCTV markings placed in prominent locations
- Change of camera targeting (data minimisation)
- The recorders are located in secure locations where appropriate measures are in place.
- Cameras installed in the Computer Room

2.10 **Ad-hoc video surveillance with drone equipment**

In order to ensure the safety and security of the residents in the Accommodation Facilities of the Reception and Identification Service, the staff and visitors, the buildings and the property assets, the Ministry of Migration and Asylum (MMA) as a configuration of the Centaur System is also provided with the possibility of **ad-hoc video surveillance with drone equipment**. The video surveillance operation with drone equipment is carried out only in exceptional cases, e.g.

Drone operators and pilots shall plan flight paths and angles at which data from drone sensors are collected in such a way as to minimise the risk of recording persons in or upon entering/exiting such buildings or locations, unless it is necessary for the purposes of the operation of the drone.

Drone operators and pilots shall plan their flight time, e.g. time of day and day of the week, in a way that minimises the risk of recording people in these locations. For example, operation close to religious buildings (within the Accommodation Facilities) during prayer times should be avoided, unless necessary for the purposes of the drone's operation.

Wherever possible, drone operators and pilots wishing to fly close to sensitive areas should inform the responsible representatives of these areas of the details of their operation and remain visible at all times.

Where special categories of personal data are likely to be collected during a drone flight over or close to sensitive areas, operators and pilots shall ensure that they act on an appropriate legal basis in accordance with Articles 9 and 10 of the GDPR.

Drone operators and pilots shall plan and perform drone flights in a manner that minimises the collection of personal data to the personal data necessary for the purposes of the drone's operations.

Drone operators and pilots shall seek to record the minimum amount of personal data and the minimum quality of personal data required for the purposes of the drone's operation. This requirement extends to the type of sensors used, their power, the type of data collected, and the type of flight path selected.

To minimise the personal data collected and the degree of privacy intrusion, pilots and drone operators shall:

- fly the drone in such a way as to collect and/or record as little data as possible about uninvolved persons on the ground;
- use lower-end sensors or adjust data quality through software controls;
- control which drone sensors are activated during flight and when;
- control when data are recorded and when they are transmitted;
- record images instead of video;
- use a secure live stream instead of data recording;
- use alternative solutions to photographic imaging, e.g. thermal imaging;
- fly at higher or lower altitudes, depending on the circumstances, to minimise the impact on people on the ground.

When a drone flight takes place near uninvolved people and especially when it takes place over or close to private or sensitive areas, the drone equipment shall have software capabilities to control:

- the sensors that are activated, e.g. optical, thermal, audio, geolocation and when the sensors are activated or deactivated during flight;
- the direction to which the drone's sensors are pointing or the angle at which they are operating;
- the quality of the data (e.g. resolution, sensor sensitivity) being recorded; and/or
- when the data collected are recorded and when they are not.

Drone pilots are trained and able to operate the selected drone equipment in a safe and efficient manner and to control it in a manner that minimises the personal data recorded to the minimum necessary for the purpose of the drone's operation.

3. Which MMA infrastructures are under surveillance?

CONTROLLED ACCESS FACILITY FOR TEMPORARY ACCOMMODATION OF ASYLUM SEEKERS AGIA ELENI

CONTROLLED ACCESS FACILITY FOR TEMPORARY ACCOMMODATION OF ASYLUM SEEKERS ALEXANDRIA
RECEPTION AND IDENTIFICATION CENTRE (RIC) DIAVATA
CONTROLLED ACCESS FACILITY FOR TEMPORARY ACCOMMODATION OF ASYLUM SEEKERS DRAMA
CONTROLLED ACCESS FACILITY FOR TEMPORARY ACCOMMODATION OF ASYLUM SEEKERS ELEFSINA
CONTROLLED ACCESS FACILITY FOR TEMPORARY ACCOMMODATION OF ASYLUM SEEKERS FILIPPIADA
RECEPTION AND IDENTIFICATION CENTRE (RIC) FYLAKIO
CONTROLLED ACCESS FACILITY FOR TEMPORARY ACCOMMODATION OF ASYLUM SEEKERS KATSIKA
CONTROLLED ACCESS FACILITY FOR TEMPORARY ACCOMMODATION OF ASYLUM SEEKERS KAVALA
KERANIS BUILDING
CONTROLLED ACCESS FACILITY FOR TEMPORARY ACCOMMODATION OF ASYLUM SEEKERS CORINTH
CLOSED CONTROLLED ACCESS CENTRE (CCAC) KOS
CONTROLLED ACCESS FACILITY FOR TEMPORARY ACCOMMODATION OF ASYLUM SEEKERS KOUTSOCHERO
CONTROLLED ACCESS FACILITY FOR TEMPORARY ACCOMMODATION OF ASYLUM SEEKERS KYLLINI
CONTROLLED ACCESS FACILITY FOR TEMPORARY ACCOMMODATION OF ASYLUM SEEKERS LAGKADIKIA
CLOSED CONTROLLED ACCESS CENTRE (CCAC) LEROS
RECEPTION AND IDENTIFICATION CENTRE (RIC) MALAKASA
CONTROLLED ACCESS FACILITY FOR TEMPORARY ACCOMMODATION OF ASYLUM SEEKERS MALAKASA
CONTROLLED ACCESS FACILITY FOR TEMPORARY ACCOMMODATION OF ASYLUM SEEKERS OINOFYTA

CONTROLLED ACCESS FACILITY FOR TEMPORARY ACCOMMODATION OF ASYLUM SEEKERS POLYKASTRO
CONTROLLED ACCESS FACILITY FOR TEMPORARY ACCOMMODATION OF ASYLUM SEEKERS PYRGOS
CONTROLLED ACCESS FACILITY FOR TEMPORARY ACCOMMODATION OF ASYLUM SEEKERS RITSONA
CLOSED CONTROLLED ACCESS CENTRE (CCAC) SAMOS
CONTROLLED ACCESS FACILITY FOR TEMPORARY ACCOMMODATION OF ASYLUM SEEKERS SCHISTO
CONTROLLED ACCESS FACILITY FOR TEMPORARY ACCOMMODATION OF ASYLUM SEEKERS SERRES
CONTROLLED ACCESS FACILITY FOR TEMPORARY ACCOMMODATION OF ASYLUM SEEKERS SINTIKI
CONTROLLED ACCESS FACILITY FOR TEMPORARY ACCOMMODATION OF ASYLUM SEEKERS THIVA
CONTROLLED ACCESS FACILITY FOR TEMPORARY ACCOMMODATION OF ASYLUM SEEKERS VAGIOCHORI
CONTROLLED ACCESS FACILITY FOR TEMPORARY ACCOMMODATION OF ASYLUM SEEKERS VEROIA
CONTROLLED ACCESS FACILITY FOR TEMPORARY ACCOMMODATION OF ASYLUM SEEKERS VOLOS

- Only authorised permanent staff of the MMA, the contractor security company and the Hellenic Police have access to the cameras and the register.

There are no cameras elsewhere where privacy is expected, such as individual offices, leisure areas, toilet facilities etc. The location of the cameras was carefully reviewed to ensure that they minimise the monitoring of areas that are not relevant to the intended purposes.

4. What personal information do we collect and for what purpose?

4.1. **Brief description and detailed technical specifications for the system.** The video surveillance system is a mixed system consisting of static cameras and PTZ cameras. It digitally records images and is equipped with motion detection. It records every movement in the coverage areas, along with the time, date and location. All cameras operate 24 hours a

day, seven days a week. The image quality in most cases allows the identification of persons in the areas covered by the camera (see guidelines, section 6.4). The fixed cameras are pre-configured and cannot be moved by the operators or focus. PTZ cameras can be controlled by the operators. Authorisation to modify the targeting and recording parameters is only given to the Installation Operator – Supervisor.

No high-tech or intelligent monitoring techniques are used (see section 6.9 of guidelines); the system is not interconnected with other systems as a physically isolated network is used (section 6.10); there is no internet connection or access and covert surveillance(section 6.11), sound recording or talking CCTV are not used (section 6.12).

4.2. **Purpose of surveillance.** The MMA uses the video surveillance system for the sole purpose of ensuring the safety of those staying in the accommodation facilities, the staff working therein, the means and infrastructure and access control. The video surveillance system helps to control access to the building and ensures the security of the accommodation facilities, the safety of residents, staff and visitors, as well as the property and information located or stored on the premises. It complements other physical security systems, such as physical access control systems and intrusion control systems. It is part of measures to support wider security policies and helps prevent, deter and, if necessary, investigate unauthorised physical access, including unauthorised access to secure areas, such as protected offices, infrastructures of Information systems or operational Information. In addition, video surveillance helps to prevent, detect and investigate theft of equipment or property belonging to the Greek State, visitors or staff, as well as threats to the safety of residents, visitors or staff working in the office (e.g. fire, attack on life).

4.3. **Restriction of purpose.** The system is not used for any other purpose, for example, it is not used to monitor the work of employees or to track their arrival at work. The system is used as an investigative tool (except for the investigation of security incidents, such as theft or unauthorised access) only in exceptional cases, the images may be transferred to investigative bodies (Hellenic Police, Public Prosecutor's Office) as part of a formal disciplinary or criminal investigation, as described in section 6.5 below (see paragraphs 5.7, 5.8 and 10.3 of guidelines).

4.4. **No ad hoc surveillance is foreseen.** No ad hoc surveillance is foreseen (see guidelines , section 3.5).

4.5. **Internet cameras.** Internet cameras are not allowed (see section 5.10 of guidelines).

4.6. **No special data categories have been collected.** No special data categories are collected (section 6.7 of guidelines).

5. **What is the legal basis for video surveillance?**

The main or general legal basis for the processing of the video surveillance is the performance of a task carried out in the public interest in the exercise of official authority (Art. 6 (1)(e) GDPR] while the processing of special categories of (biometric) data takes place for reasons of substantial public interest (Article 9 (2)(g) GDPR), (2)(g) GDPR) under the

Dublin III Regulation or the Immigration Code, while the Closed Controlled Access Centres (CCAC) constitute 'critical infrastructures of the State' in conjunction with Law 4624/2019 taking into account guideline 1/2011 of the HDPA and guidelines 3/2019 of the EDPB. The public interest consists in the need to protect the critical infrastructures belonging to the Greek state, the human and information resources held within them against illegal acts. In addition to the above, with a special sense of responsibility and respect for people, the above framework of protection includes the safety of life, physical integrity, health and property of the residents, our staff, associates and visitors in general who enter the monitored area. Data collection is restricted to image capture only and in places where we have assessed that there is an increased likelihood of unlawful acts to be committed and increased protection of persons and goods, e.g. at entry points, without focusing on places where the privacy of the persons whose image is taken may be unduly restricted, including their right to respect for personal data.

6. **Who has access to information and to whom is it disclosed?**

6.1. **Security staff and external partners – security guards.** The recorded video is accessible only to authorised employees of the MMA and not to all security and guarding staff. The live video in the Signal Receiving Centre is accessible by the security guards on duty. These guards belong to a contractor specialised company providing security, maintenance services and technical support for the systems, with the contract awarding option provided for in Article 14 (1) of Law 3907/2011. The contractor company is committed by means of a written contract ensuring the confidentiality and security of the processing (Processor).

6.2. **Access rights.** The MMA's security policy for video surveillance (see section 7 below) clearly specifies and documents in writing who has access to the video surveillance footage and/or the technical architecture of the video surveillance system, for which purpose, and the content of the access rights. More specifically, the document clarifies who has the right to:

- show the video in real time;
- view the recorded footage; or
- copy the visual recording file;
- download the visual recording file;
- erase the visual recording file; or
- modify the settings of any part of the footage.

6.3. **Data protection training.** All MMA staff with access rights, including outsourced personnel have been given at least one data protection training. Training is provided to each new staff member and periodic seminars on data protection awareness and compliance matters are held at least once every two years for all staff with access rights (see section 8.2 of guidelines).

6.4. **Confidentiality obligations.** After the training, each member of the contractor's security staff is bound by a confidentiality agreement. The agreement is also signed by the Processor (project Contractor) providing the external associates. (see section 8.3 of guidelines).

6.5. **Transfers and disclosures.** All transfers and disclosures of Data outside the secure facility are documented and subject to a rigorous assessment of the necessity of the transfer and the compatibility of the purposes of the transfer with the initial purpose of security control and processing access (see chapter 10 of the guidelines). The transfer policy is governed by the GDPR 679/2016. (see section 10.5 and 7.2 of guidelines). The opinion of the MMA's DPO shall be sought in all cases.

Prosecuting and Police Authorities may have access as part of an investigation or prosecution of criminal offences.

In exceptional cases, access may also be granted to:

- the Public Prosecutor by order of the same
- the Competent Supervisory Authority
- those conducting a formal internal investigation or disciplinary procedure within the Company,

provided that the transfers can reasonably be expected to assist in the investigation or prosecution of a disciplinary or criminal offence. Requests for data collection are not served.

7. **How do we protect and safeguard information?**

In order to protect the security of the video surveillance system, a certain procedure has been established. This process includes instructions to the department or the external Security Services company that oversees the screens at the facilities' entrance.

Among other things, the following reasonable security measures shall be taken:

- Secure areas, protected with physical security measures, host the servers that store the recorded images. Network firewalls protect the logical perimeter of the IT infrastructure. The main computer systems holding the data have increased security and access control measures.
- Administrative measures include the obligation for each member of staff - external associate with access to the system (including those maintaining the equipment and systems) to take separate security measures.
- Users are granted access rights only to the level strictly necessary for the performance of their tasks.
- Only the system operator specifically designated by the controller for this purpose may grant, modify or revoke any access rights of persons.
- Any assignment, modification or removal of access rights shall be carried out in accordance with the criteria set forth in the video surveillance security policy.

- The video surveillance security policy contains an up-to-date list of all people with access to the system at any given time and details their access rights.

8. **How long do we keep the data for?**

The visual recordings of the surveillance cameras are kept for 15 days after which they are automatically deleted. In the event that we discover an incident during that period, we will isolate part of the video and keep it for up to one (1) more month in order to investigate the incident and initiate legal proceedings to defend our legal interests, while if the incident concerns a third party we will keep the video for up to three (3) more months. In the event of files and audiovisual data stored or downloaded in real time not resulting in the occurrence of an event falling within the intended purpose, the data shall be destroyed within fifteen (15) calendar days at the latest, subject to more specific provisions of the applicable legislation as in force for specific categories of data controllers. In the event of an incident relating to the purpose of processing, the MMA shall keep the recordings, in which the specific incident has been recorded, in a separate file for three (3) months. After the above period, the MMA may keep the data for a longer specific period only in exceptional cases where the incident requires further investigation. In this case, the MMA is obliged to inform the Authority of the necessary period of time to keep such downloads. If any video needs to be stored to further investigate or prove a security incident, it may be kept as necessary and only with the permission of the Data Protection Officer. The request for their retention shall be strictly documented and the need for retention shall be periodically reviewed, upon recommendation of the Data Protection Officer.

The system is also monitored live by the security staff at the reception of each accommodation facility and in the security building on a 24/7 basis.

9. **How do we provide information to the public?**

9.1. Multi-layer approach: We provide information to the public about the video-surveillance in an effective and comprehensive manner (see guidelines, section 11). To this end, we follow a multi-layer approach, which consists of a combination of the following two methods:

- On-the-spot notices (information signage) to inform the public that monitoring is taking place and to provide them with meaningful information about the processing; and
- surveillance policy leaflets are also available at the reception of the accommodation facilities. A telephone number and email address are provided for further questions.
- We also provide on-the-spot notices next to the areas being monitored. We placed a notice at the main entrance, one at the reception desk, one at the entrance to the parking area and one at the side office in the yard.

The organisation's on-the-spot data protection notice is included as Attachment 8.

9.2. **Special individual notice.** In addition, individuals must also be given individual notice if they were identified on camera (for example, by security staff in a security investigation) provided that one or more of the following conditions also apply:

- the identity of the individual is noted in any files/records;
- the video recording is used against the individual;
- the video recording is kept beyond the regular retention period;
- the video recording is transferred outside the security unit; or
- the identity of the individual is disclosed to anyone outside the security unit.

Provisions of notice may sometimes be delayed temporarily, for example, if it is necessary for the prevention, investigation, detection and prosecution of criminal offences.

In all these cases, the DPO is consulted to ensure that the rights of the individual are respected.

10. **How can members of the public verify, modify or erase their information?**

The public has the right to access the personal data held and to rectify and/or complete such data. Any request for access, rectification, blocking and/or erasure of personal data should be addressed to the MMA's Data Protection Officer in charge (email: dpo@migration.gov.gr contact form: https://migration.gov.gr/epikoinonia/, 196 – 198 Thivon Avenue, P.C. 182 33, Agios Ioannis Rentis – Nikaia, Attica). You may also be contacted in case of other questions regarding the processing of personal data.

Whenever possible, the MMA will respond to a request for an investigation within 30 calendar days. If this is not possible, the applicant will be informed of the next steps and the reason for the delay within 30 days. Even in the most complex cases, access must be granted or a final reasoned reply rejecting the request must be given within one month at the latest. The MMA should do its best to respond earlier, especially if the applicant demonstrates the urgency of the request.

If explicitly requested, viewing of the images may be arranged or the applicant may receive a copy of the recorded images on a DVD or other portable storage medium (usb stick). In the event of such a request, applicants should state their identity beyond reasonable doubt (e.g. they should wear identification cards when being monitored) and, whenever possible, also specify the date, time, location and circumstances at the time of recording in the video surveillance system. They must also provide a recent clear photograph of themselves, allowing security staff to identify them from the images reviewed.

A request for access may be rejected if, for example, the restriction of access is necessary to safeguard the investigation of a criminal offence. A restriction may also be necessary to protect the rights and freedoms of other citizens/workers, for example, when other people are also present in the video and it is not possible to obtain their consent for the disclosure of their personal data or to use image processing to address the lack of consent.

11**. Right of appeal**

Every individual has the right to appeal to the Hellenic Data Protection Authority if he or she considers that his or her rights have been violated as a result of the processing of his or her personal data by the organisation. Before doing so, we recommend that people first try to contact:

- The MMA (see contact details above) and/or
- The Data Protection Officer of the MMA

Employees of the MMA may also request a review by the competent Administrative Authority under the General Staff Regulations of the MMA.

Last update: June 2024