|  |
| --- |
|  |
|  |
|  |
| Video Surveillance Policy template |
|  |
|  |
|  |
|  |

# Sample template: Video Surveillance Policy

Disclaimer: The sample Video Surveillance Policy must be checked by the Controller. GDPR compliance using this sample is his area of responsibility.

[Agency] Video Surveillance Policy

Adopted by the Director's Decision on [DD, MM, YYYY]

1. Purpose and scope of the Agency's Video Surveillance Policy

For the safety and security of its buildings, assets, staff and visitors, our Agency operates a video surveillance system. This Video Surveillance Policy, along with its attachments, describes the Agency's video surveillance system and the safeguards that the Agency takes to protect the personal data, privacy and other fundamental rights and legitimate interests of those caught on the cameras.

2. How we ensure that our video surveillance system is designed with privacy and data protection concerns in mind and is compliant with data protection law

2.1 Revision of the existing system. A video surveillance system had already been operating in our Agency before the application of the European General Data Protection Regulation (GDPR) on May 25th, 2018. Our procedures, however, have since then been revised to comply with GDPR (GDPR, Section [XX]). [link to the GDPR website]

2.2 Compliance status. The Agency processes the images and data in respect to the protection of personal data in accordance with the GDPR and the laws of [local community, organizations and bodies]. (If you deviate from any recommendations in the GDPR, this should be clearly stated and justified in your video surveillance policy.)

2.3 Self-audit. The system was subject to a self-audit. The audit report is attached as Attachment 1.

2.4 Contacts with the relevant data protection authority in the Member State. The competent data protection authority in [insert country] was informed and its concerns and recommendations were taken into account. In particular, both the on-the-spot notice and this Video Surveillance Policy are also available in [local language/s].

2.5 Director's decision and consultation. The decision to use the current video surveillance system and to adopt the safeguards as described in this Video Surveillance Policy was made by the Director of the Agency after consulting:

* The head of the Agency's security unit
* The Agency's Data Protection Officer

And the Staff Committee During this decision-making process, the Agency:

* Demonstrated and documented the need for a video surveillance system as proposed in this policy
* Discussed alternatives and concluded that the maintenance of the current video surveillance system, after the adoption of the data protection safeguards proposed in this policy, is necessary, and
* Addressed the concerns of the DPO and the Staff Committee.

2.6 Transparency. The Video Surveillance Policy has two versions, a version for restricted use and this public version available and posted on our internet and intranet sites at [internet and intranet addresses]. This public version of the Video Surveillance Policy may contain summary information with respect to particular topics or attachments. When this is the case, it is always clearly stated. Information is only omitted from the public version when the preservation of confidentiality is absolutely necessary for compelling reasons (for example, for security reasons or to preserve the confidentiality of commercially sensitive information or to protect the privacy of individuals).

2.7 Periodic reviews. A periodic data protection review will be undertaken by the security unit every two years, the first by [DD, MM, YYYY]. During the periodic reviews we will re-assess that:

* There continues to be a need for the video surveillance system
* The system continues to serve its declared purpose, and that
* Adequate alternatives remain unavailable

The periodic reviews will also cover all other issues addressed in the first report, in particular, whether our Video Surveillance Policy continues to comply with GDPR, and whether it is followed in practice (compliance audit). Copies of the periodic reports will also be attached to this Video Surveillance Policy in Attachment 1.

2.8 Privacy-friendly technological solutions. We also implemented the following privacy-friendly solutions:

[list and describe the solutions implemented]

3. What areas are under surveillance?

The video surveillance system consists of [number and type of cameras]. A map of the surveyed area with the locations of the cameras is included in Attachment 2.

Of the [# cameras, #] are located at entry and exit points of our building, including the main entrance, emergency and fire exits and the entrance to the parking lot. In addition, there is also a camera at the entrance to the stairway in the parking lot.

There are no cameras elsewhere, either in the building or outside of it. We also do not monitor any areas under heightened expectations of privacy such as individual offices, leisure areas, toilet facilities and others. The location of the cameras was carefully reviewed to ensure that they minimize the monitoring of areas that are not relevant for the intended purposes.

Monitoring outside our building on the territory of [insert name of the Member State where you are located] is limited to an absolute minimum.

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

4.1 Summary description and detailed technical specifications for the system.

The VMS is a conventional video surveillance system. It records digital video, and is equipped with motion detection. The VMS records the video whenever motion is detected by the cameras in the area under surveillance, together with time and date. All cameras operate 24 hours a day, seven days a week. The image quality in most cases allows identification of those in the camera's area of coverage. The cameras are all fixed (there are no pan-tilt-and-zoom cameras), and thus, they cannot be used by the operators to zoom in on a target or follow individuals around.

The technical specifications for the cameras and for the video surveillance system as a whole (including any software and hardware) are included in Attachment 3.

4.2 Purpose of the surveillance. The Agency uses its video surveillance system for the sole purposes of security and access control. The video surveillance system helps control access to our building and helps ensure the security of our building, the safety of our staff and visitors, as well as property and information located or stored on the premises. It complements other physical security systems such as access control systems and physical intrusion control systems. It forms part of the measures to support our broader security policies and helps prevent, deter, and if necessary, investigate unauthorized physical access, including unauthorized access to secure premises and protected rooms, IT infrastructure, or operational information. In addition, video surveillance helps prevent, detect and investigate theft of equipment or assets owned by the Agency, visitors or staff, and threats to the safety of visitors or personnel working at the office (for example, fire, physical assault).

4.3 Purpose limitation. The system is not used for any other purpose, for example, it is not used to monitor the work of employees or to monitor attendance. Neither is the system used as an investigative tool (other than investigating physical security incidents such as thefts or unauthorized access) It is only in exceptional circumstances that the recordings may be transferred to investigatory bodies in the framework of a formal disciplinary or criminal investigation as described in Section 6.5 below.

4.4 No ad hoc surveillance foreseen. We foresee no ad hoc surveillance operations for which we would need to plan at this time.

4.5 No special categories of data analyzed. We do not analyze video footage concerning special categories of data.

5. What is the lawful ground and legal basis of the video surveillance?

The use of our video surveillance system is necessary for the management and functioning of our Agency (for the security and access control purpose described in Section 4.2 above). Therefore, we have a lawful ground for the video surveillance.

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

6.1 In-house security staff and outsourced security-guards. Surveillance recordings are accessible to our in-house security staff only. Live video is also accessible to security guards on duty. These security guards work for an outsourced security company.

The contract with this security company is included in Attachment 4.

6.2 Access rights. The Agency's Security Policy for Video Surveillance (see Section 7 below and Attachment 7) clearly specifies and documents who has access to the surveillance video and/or the servers that run the VMS, for what purpose and what those access rights consist of. In particular, the document specifies, per device (camera, microphone, speaker, metadata), who has the right to:

* View the real-time video
* View the recorded video
* Make snapshots
* Make exports of video
* Hand out exports to people outside the company
* Delete or remove devices (cameras)
* Delete video

6.3 Data protection training. All personnel with access rights, including the outsourced security guards, were given their first data protection training on [DD, MM, YYYY]. Training is provided for each new member of the staff and periodic workshops on data protection compliance issues are carried out at least once every year for all staff with access rights.

6.4 Confidentiality undertakings. After the training, each staff member also signed a confidentiality undertaking. This undertaking was also signed by the outsourced company. Copies of these confidentiality undertakings are attached as Attachment 5.

6.5 Transfers and disclosures. All transfers and disclosures outside the security unit are documented and subject to a rigorous assessment of the necessity of such transfer and the compatibility of the purposes of the transfer with the initial security and access control purpose of the processing.

The register of retention and transfers is included in Attachment 6. The DPO of the Agency is consulted in each case. [If you have routine transfers which are made without the involvement of the DPO, please describe your policy in detail in this Video Surveillance Policy.]

No access is given to management or human resources. [If this is not the case, please provide illustrative examples of such transfers. Please also describe your rules on what can be transferred to whom and under what circumstances.]

Local police may be given access if needed to investigate or prosecute criminal offenses. [Please also describe your rules on what can be transferred to whom and under what circumstances.] Incidents are documented in the incident log, which is kept for [X] years.

Under exceptional circumstances, access may also be given to:

* The European Anti-fraud Office (“OLAF”) in the framework of an investigation carried out by OLAF
* The Commission's Investigation and Disciplinary Office ("IDOC") in the framework of a disciplinary investigation, under the rules set forth in Annex IX of the Staff Regulations of Officials of the European Communities
* Those carrying out a formal internal investigation or disciplinary procedure within the organization, provided that it can be reasonably expected that the transfers may help investigation or prosecution of a sufficiently serious disciplinary offense or a criminal offense. No requests for data mining are accommodated.

7. How do we protect and safeguard the information?

In order to protect the security of the video surveillance system, including personal data, a number of technical and organizational measures have been put in place.

These are detailed in a processing-specific security policy ("Security Policy for Video Surveillance"), which is attached as Attachment 7.

Among others, the following measures are taken:

* Secure premises, protected by physical security measures, host the servers storing the media recorded; network firewalls protect the logic perimeter of the IT infrastructure; and the main computer systems holding the data are security hardened.
* Administrative measures include the obligation of all outsourced personnel having access to the system (including those maintaining the equipment and the systems) to be individually security cleared.
* All staff (external and internal) signed non-disclosure and confidentiality agreements.
* Access rights to users are granted to only those resources which are strictly necessary to carry out their jobs.
* Only the system administrator specifically appointed by the Data Controller for this purpose is able to grant, alter or annul any access rights of any persons. Any provision, alteration or annulment of access rights is made pursuant to the criteria established in the Security Policy for Video Surveillance (see Attachment 7).
* The Security Policy for Video Surveillance contains an up-to-date list of all persons having access to the system at all times and describes their access rights in detail.

8. How long do we keep the data?

The recorded media are retained for a maximum of [X] days. Thereafter, all media are deleted. If anything needs to be stored to further investigate or evidence a security incident, they may be retained as necessary. Their retention is rigorously documented and the need for retention is periodically reviewed. A copy of the register of retention and transfers is included in Attachment 6.

The system is also monitored live by the security guard in the downstairs building reception 24 hours a day.

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.

To this end, we follow a multi-layer approach, which consists of a combination of the following two methods:

* On-the-spot notices to alert the public to the fact that monitoring takes place and provide them with essential information about the processing
* We post this Video Surveillance Policy on our intranet and also on our internet sites for those wishing to know more about the video surveillance practices of our organization.

Print-outs of this Video Surveillance Policy are also available at our building reception desk and from our security unit upon request. A phone number and an email address are provided for further inquiries.

We also provide on-the-spot notice adjacent to the areas monitored. We placed a notice near the main entrance, the elevator entrance in the parking lot and at the entry to the parking lot.

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

9.2 Specific 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:

* Their identity 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
* The identity of the individual is disclosed to anyone outside the security unit

Provision of notice may sometimes be delayed temporarily, for example, if it is necessary for the prevention, investigation, detection and prosecution of criminal offenses (Other exceptions under Article 13 of the GDPR may also apply in exceptional circumstances). The Agency's DPO is consulted in all such cases to ensure that the individual’s rights are respected.

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

Members of the public have the right to access the personal data we hold on them and to correct and complete such data. Any request for access, rectification, blocking and/or erasing of personal data should be directed to Ms/Mr \_\_\_\_\_\_, Head of Unit \_\_ [email address and telephone number]. He or she may also be contacted in case of any other questions relating to the processing of personal data.

Whenever possible, the security unit responds to an inquiry in substance within [X] calendar days. If this is not possible, the applicant is informed of the next steps and the reason for the delay within [X] days. Even in the most complex of cases, access must be granted or a final reasoned response must be provided rejecting the request within three months at the latest. The unit must do its best to respond earlier, especially if the applicant establishes the urgency of the request.

If specifically requested, a viewing of the images may be arranged or the applicant may obtain a copy of the recorded media on a DVD or other media. In case of such a request, the applicants must indicate their identity beyond doubt (for example, they should bring identity cards when attending the viewing) and, whenever possible, also designate the date, time, location and circumstances when they were caught on cameras. They must also provide a recent photograph of themselves that allows the security staff to identify them from the images reviewed.

At this time, we do not charge applicants for requesting a viewing or a copy of their recorded images. However, we reserve the right to charge a reasonable amount in case the number of such access requests increases.

An access request may be refused when an exemption under Article 15 of GDPR applies in a specific case. For example, following a case-by-case evaluation we may have to conclude that restricting access may be necessary to safeguard the investigation of a criminal offense. A restriction may also be necessary to protect the rights and freedoms of others, for example, when other people are also present on the images, and it is not possible to acquire their consent to the disclosure of their personal data or to use image-editing to remedy the lack of consent. In these cases it has to be taken in account to mask out other people in the video using third-party tools before rejecting a request of a data subject.

11. Right of recourse

Every individual has the right of recourse if they consider that their rights under the GDPR have been infringed as a result of the processing of their personal data by the Agency. Before doing so, we recommend that individuals first try to obtain recourse by contacting:

* The head of the security unit (see contact details above), and/or
* The data protection officer of the Agency [insert name, telephone number and email address]

Staff members may also request a review from their appointing authority.

[Details of internal recourse procedure, including timeliness and contact details.]\* \* \*

Attachments to the Video Surveillance Policy:

* The audit report is attached as Attachment 1. Attachment 1 will also contain the periodic reviews.
* A map with the locations of the cameras is included in Attachment 2.
* The technical specifications for the cameras and for the video surveillance system as a whole (including any software and hardware) are included in Attachment 3.
* The contract with the outsourced security company is included in Attachment 4.
* Copies of the confidentiality undertakings are attached as Attachment 5.
* The register of retention and transfers is included in Attachment 6.
* In order to protect the security of the video surveillance system, including personal data contained in it, a number of technical and organizational measures have been put in place. These are detailed in a processing-specific security policy ("Security Policy for Video Surveillance"), which is attached as Attachment 7.
* The Agency's on-the-spot data protection notice is included as Attachment 8.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | |  |  |  |  | | --- | --- | --- | --- | |  |  |  |  | |
|  | Milestone Systems is a leading provider of open platform video management software; technology that helps the world see how to ensure safety, protect assets and increase business efficiency. Milestone enables an open platform community that drives collaboration and innovation in the development and use of network video technology, with reliable and scalable solutions that are proven in more than 150,000 sites worldwide. Founded in 1998, Milestone is a stand-alone company in the Canon Group. |