Privacy statement and policy on the video-surveillance at the BEREC Office

This video-surveillance policy defines the practical implementation of video-surveillance at the BEREC Office, while at the same time protecting the personal data, privacy and other fundamental rights and legitimate interests of data subjects.

1. Scope

The video-surveillance policy covers video material produced by surveillance system in the BEREC Office’s premises.

The recording and broadcasting of events, meetings and trainings as well as video-conferencing and video-entry systems (door-phones) are excluded from the scope.

2. Description

The maintenance of the current video-surveillance system, after the adoption of the data protection safeguards proposed in this policy, is necessary and proportionate for the purposes described further in this document.

Video-monitoring is an important tool in protecting BEREC Office’s premises, assets, staff, visitors and the information stored and processed therein. It complements other physical security systems such as access control system and physical intrusion control system. It helps prevent, deter and, if necessary, investigate unauthorized physical access. In addition, video-surveillance helps prevent security incidents, detect them when they happen and to investigate them.

The video-surveillance may also be used to monitor evacuation of the building and to complement the access control system, especially outside the office hours.

Video-surveillance will not be used for performance assessment and appraisal of the staff. The data shall only be used in disciplinary proceedings in exceptional cases, when the images captured demonstrate a physical security incident or criminal behaviour.

Use of the video-surveillance system at the BEREC Office for the sole purpose of security and access control described above is necessary for the management and functioning of the BEREC Office, therefore there is a legitimate ground for the video-surveillance.

The BEREC Office processes the images in accordance with both the Regulation (EC) 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the European institutions and
2.1. Coverage

The video-surveillance system consists of 3 (three) fixed cameras. All cameras are located at entry and exit points of the premises, including emergency exits.

There are no cameras elsewhere. Those cameras do not monitor 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 minimise the monitoring of areas that are not relevant for the intended purposes.

2.2. Used technology

All cameras operate 24 hours a day, 7 days a week.

The image quality in most cases allows identification of individuals. All monitoring cameras are recording ones, but no sound recording takes place.

Cameras record any movement detected by the cameras in the area under surveillance, together with time, date and location.

The video-surveillance system is not interconnected to any other video-surveillance system.

Covert video-surveillance, infrared cameras and ad hoc monitoring will not be used.

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.

2.3. Responsibilities and access rights

The Head of Administration and Finance is responsible for the implementation of this policy. He/she will approve any exceptions and consult the Data Protection Officer where appropriate. In case of negative opinion, the exceptional action shall be interrupted.

The number of users of the system is kept to an indispensable minimum, and includes:

• Logistics and Security Assistant responsible for system management issues, and with full access to the system. He/she can read, copy, move and delete video material. He/she is responsible for the safe retention and deletion of the files.

• The external security guards watch live video. They do not have direct access to video footage (files recorded by cameras). He/she will inform the Logistics and Security Assistant of any of the following:
  - suspected abuse of the video-surveillance system;
  - cameras which are not working, poorly placed or focused or otherwise do not increase security or put data protection at risk;
  - suspected security incidents where video material should be kept after the normal retention period;
  - requests of public authorities to access or transfer the stored video footage.

2.4. Storage

The video-surveillance system is a standalone and recordings will thus be stored on a system not connected to BEREC Office’s local area network (LAN).

No back-up copies of the video footage files are taken.

Access logging is in place. It enables to monitor the usage and detect misuse. The users are informed about this.

The servers storing the recorded images are located within secure premises and protected by physical security measures.

2.5. Retention period

The normal retention period of a video-recording is 14 calendar days. The period has been defined based on the experiences gathered by operating the system.

If a security incident is investigated, the Head of Administration and Finance can decide on a longer retention period on case-by-case basis.

A register is kept by the Logistics and Security Assistant of all video-recording material retained after the normal retention period.

After 14 calendar days the camera-recording files shall be automatically and permanently deleted.
2.6. Transfers and disclosure of video material

All transfer and disclosure requests are 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. This assessment is done by the Head of Administration and Finance who will enter the request and his/her decision in a registry. Requests from police authorities (signed by a police officer having a sufficiently high rank), a public prosecutor or a court of law can be considered only if needed to investigate or prosecute criminal offences and when a formal written request is made according to the requirements of the applicable national law regarding form and consent. The disclosure shall only take place if another organisation established under Latvian law would also be required or at least permitted to make the disclosure under similar circumstances. General requests for data mining purposes are explicitly excluded. On official request, the Head of Administration and Finance can also authorise a police official to see a live replay of video-monitoring material in the BEREC Office’s premises without transferring the file.

In exceptional cases, upon official request, video footage may also be transferred to the European Anti-Fraud Office (OLAF), the European Ombudsman, The Internal Audit Service (IAS), the European Court of Auditors (ECA) or the European Data Protection Supervisor (EDPS).

On the duly justified request of the investigator appointed by the Vice Chair, video footage may also be transferred for the purpose of an administrative inquiry and the possible follow-up during disciplinary proceedings when the images captured demonstrate a physical security incident or criminal behaviour. Following this procedure the transferred video footage might consequently be disclosed to the investigator, the Vice Chair, the person nominated coordinate the administrative inquiries, the person assigned by the Vice Chair to hold the hearing, the Disciplinary Board, the Legal Officer or any other staff member directly involved in the administrative inquiry or disciplinary proceedings.

The Head of Administration and Finance shall perform a mandatory consultation of the Data Protection Officer of the BEREC Office regarding all transfer requests.

2.7. Process for handling access requests

Any requests by a data subject to receive access to his/her personal data processed via the video-surveillance system shall be addressed to the Head of Administration and Finance, who will handle the request without undue delay and in line with the principles of ethical administrative behaviour, while at the same time safeguarding the rights of third parties present on the same recordings.

If a request is denied, the individual making the request is informed about his/her right to have recourse to the EDPS.
The same procedure applies when exercising any other right of the data subject.

2.8. Assessment and audit of the system

An adequacy and compliance audit of the video-surveillance system shall be performed once every two years and also every time a significant change in the circumstances warrants a review. The results shall be summarised in a written audit report.

2.9. Interest group involvement

The opinion of the Staff Committee and the Data Protection Officer (DPO) of the BEREC Office will be sought when major changes are proposed to this procedure.

The Data Protection Authority of the Republic of Latvia will be notified of cases where the video-surveillance extends to the Member State’s territory.

Simultaneously with adopting the video-surveillance policy, the EDPS is notified of the compliance status by sending them a copy of the policy and related documents.

2.10. Information to data subjects

An on-the-spot notice announces that video-surveillance is in place at the entrance of the BEREC Office’s premises. It alerts the public to the fact that monitoring takes place and provide them with essential information about the processing.

The video-surveillance policy shall be posted on the BEREC Office website for those who wish to receive more information. In addition, printed hard-copies of the policy shall be made available at the reception of the BEREC Office.

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 record is kept beyond the regular retention period;
- the recording is transferred outside the security unit, or
- the identity of the individual is disclosed to any individual 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 offences. The DPO of the

---

2 http://www.dvi.gov.lv
BEREC Office is consulted in all such cases to ensure that the individual’s rights are respected.

**2.11. Confidentiality of information**

Everyone granted with an access to the video-monitoring system shall sign a specific confidentiality undertaking, indicating that they shall not record, and copy, modify, re-direct or otherwise process the video-stream. Confidentiality obligations apply to the information obtained through the video-surveillance system.

A prior approval of the Head of Administration and Finance is required before information on footage is revealed to an outsider.

**2.12. Training**

The security staff, including the external security guards shall be offered training regarding the proper use of the surveillance system and on Data Protection obligations related to this policy.

**2.13. Recourse to the EDPS**

Every individual has the right of recourse to the EDPS (edps@edps.europa.eu) if they consider that their rights under the Regulation (EC) 45/2001 have been infringed as a result of the processing of their personal data by the BEREC Office. Before doing so, it is recommended that individuals first try to obtain recourse by contacting the Data Protection Officer of the BEREC Office at dpo@berec.europa.eu.